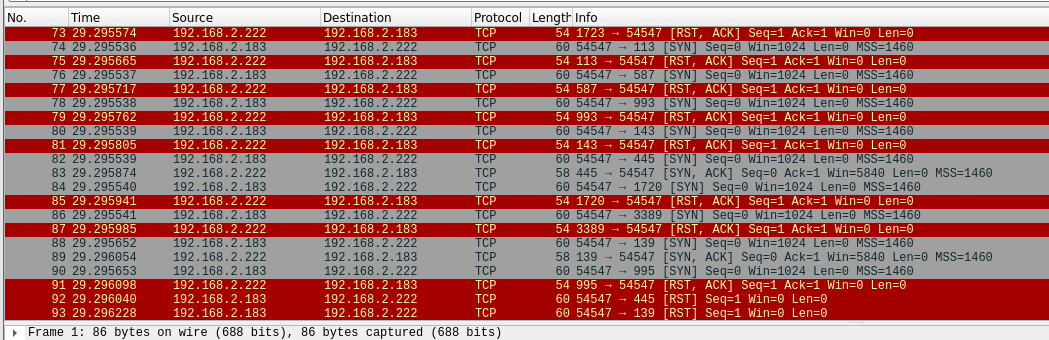
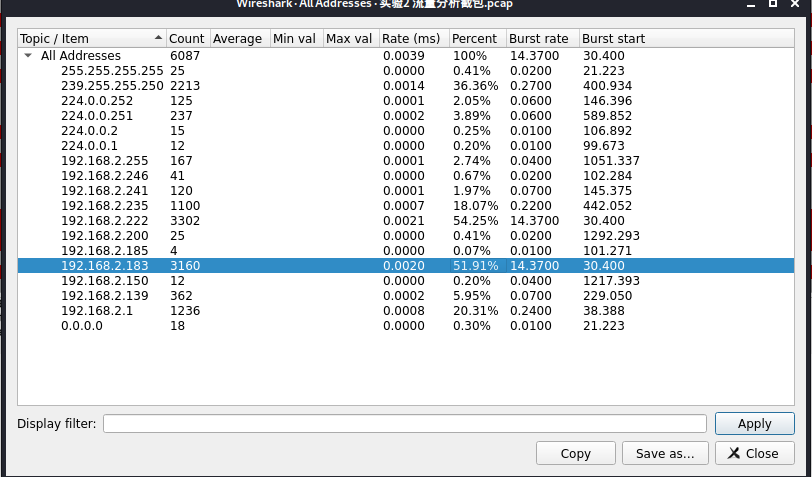
（1）攻击主机的信息

攻击机IP为192.168.2.183，端口为54547。

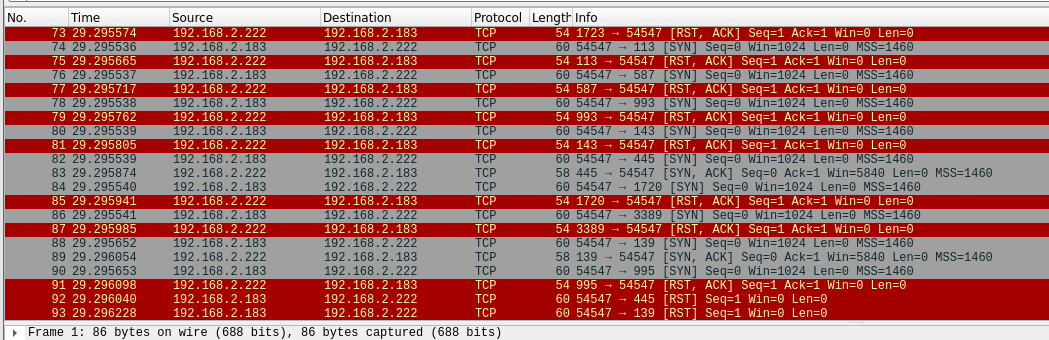


（2）流量分析的过程，以及分析出来的攻击步骤

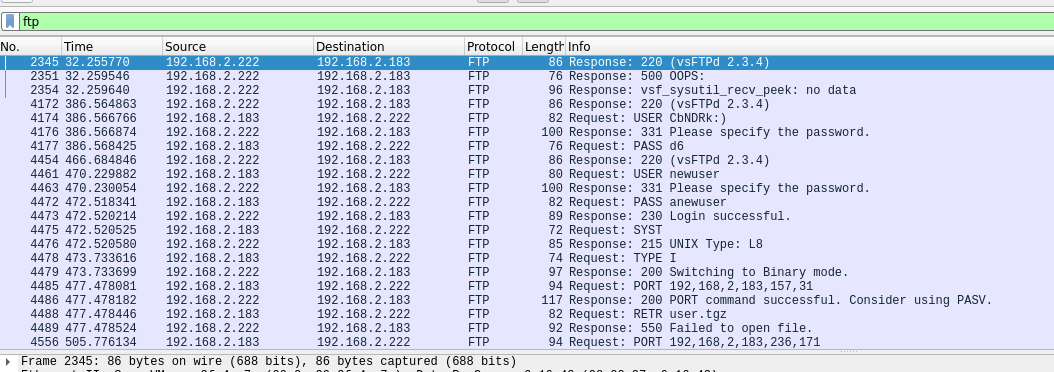
先利用IPv4统计信息，得出主要主机信息



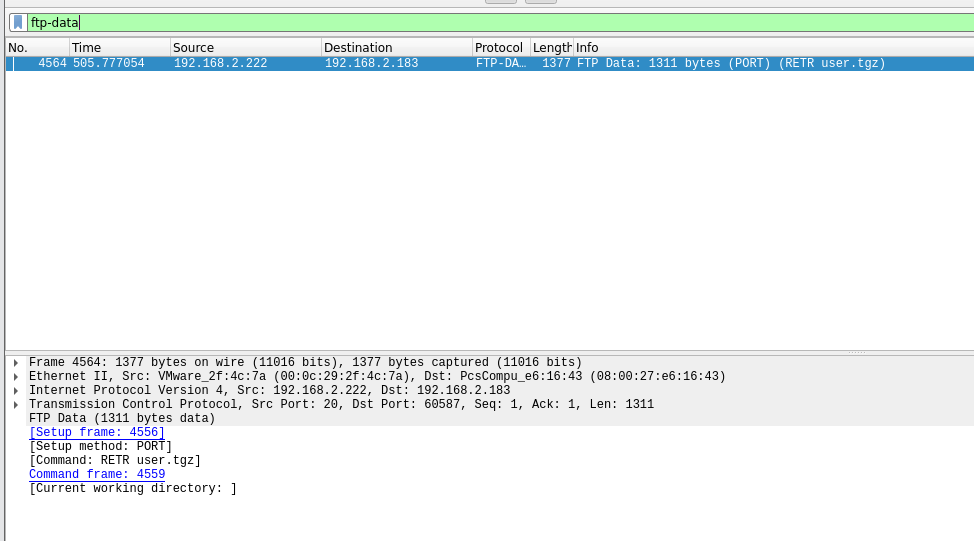
分析大量的TCP连接，得出在进行端口扫描。靶机IP为192.168.2.222，攻击机IP为192.168.2.183，端口为54547。



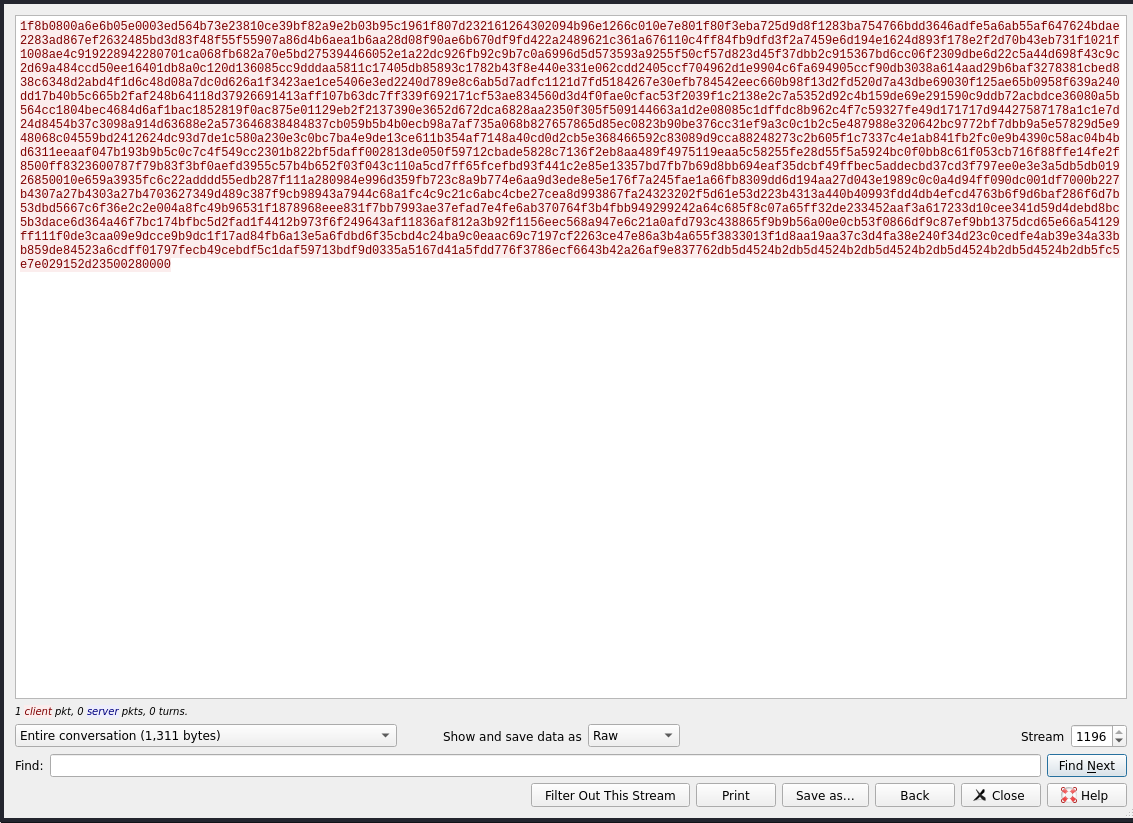
查看ftp协议相关的报文，猜测可能利用vsFTPd相关漏洞。



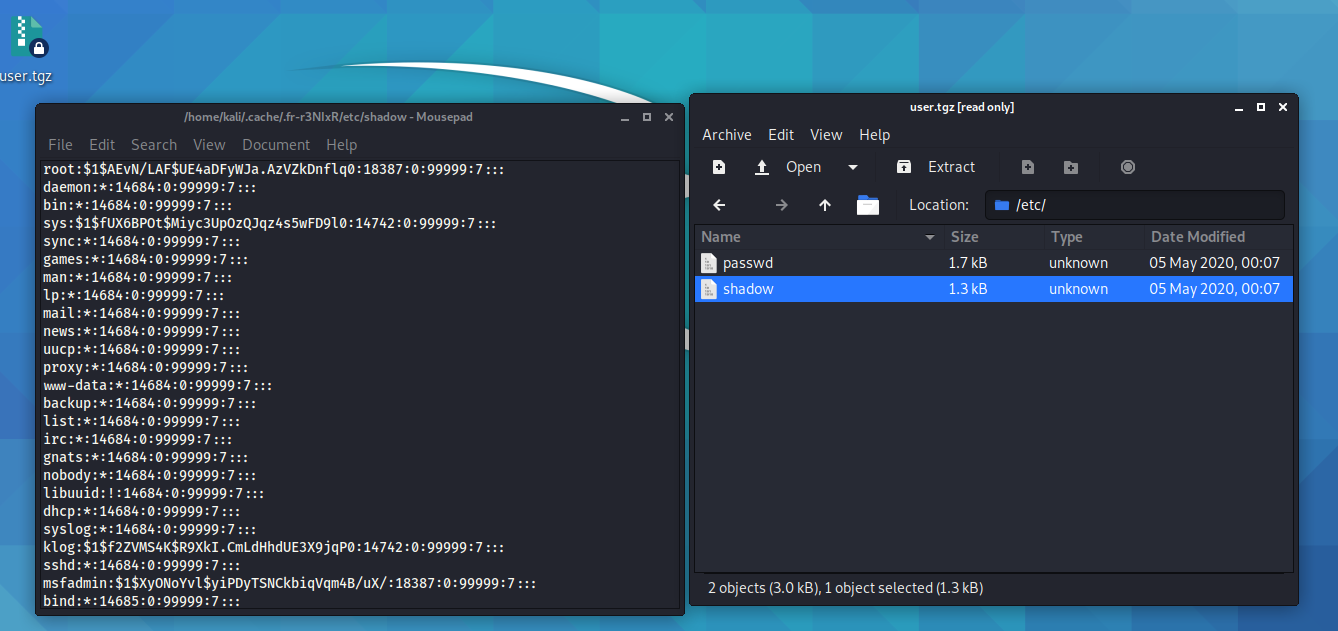
通过ftp-data过滤，查看靶机发送给攻击机的文件。



跟踪TCP流，保存信息。



打开文件，发现攻击机获得了靶机上的shadow文件。



分析出来的攻击步骤：

攻击机利用了靶机上的vsFTPd 2.3.4的后门漏洞，建立了一个远程shell，并通过ftp传输获得靶机上的shadow文件。

（3）破解出来的root口令

使用hashcat对root用户密码执行解密，获得root用户密码adminmsf。

