第六题：

知识点：wireshark下对pcap包进行分析

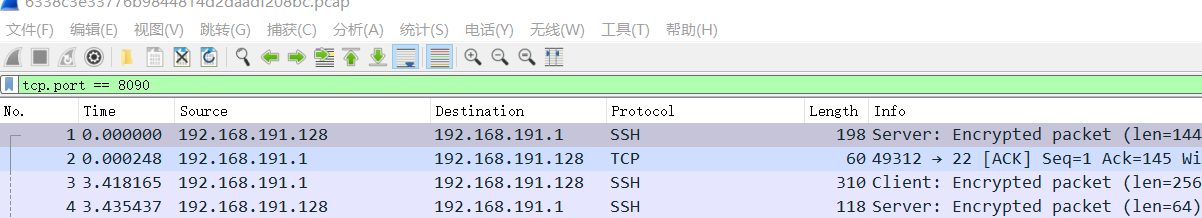
wireshark过滤规则以及显示规则

http://blog.csdn.net/blues1021/article/details/48031099

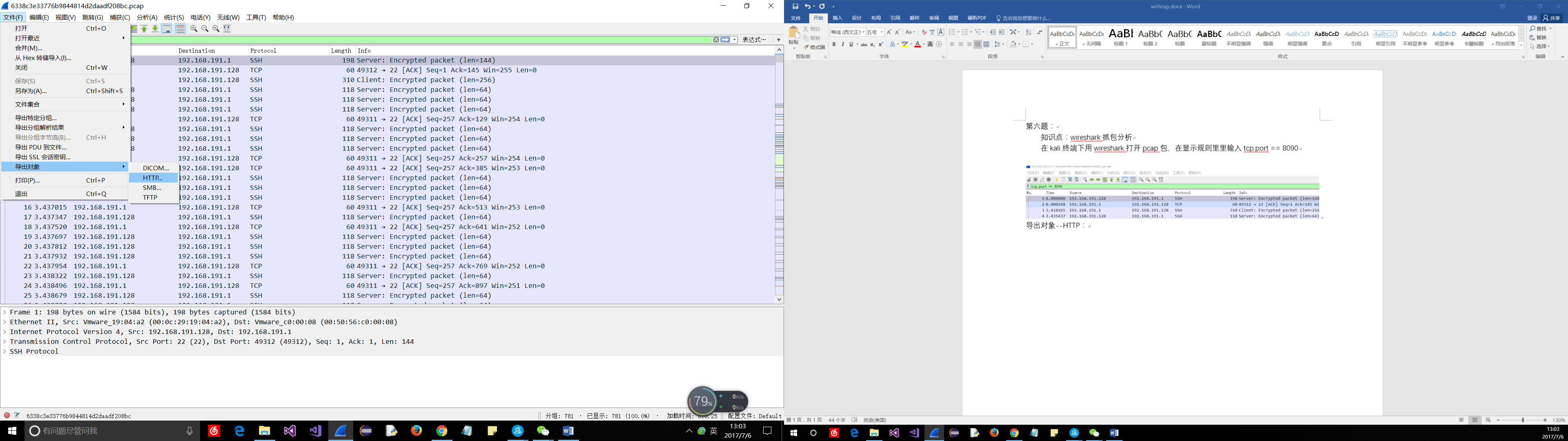
拓展：linux下使用tcpdump抓包

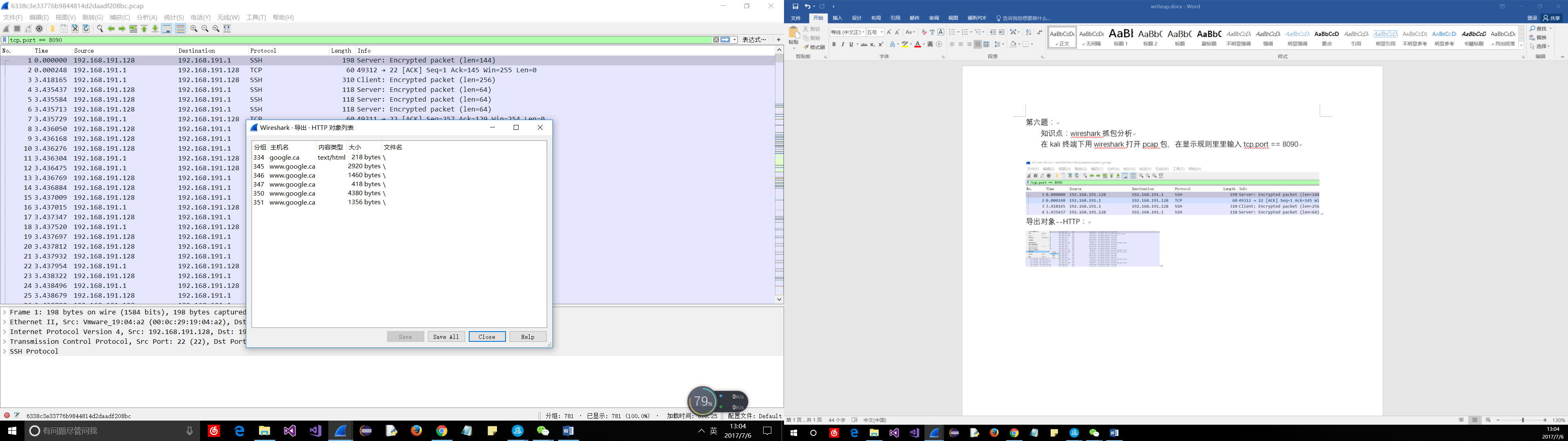
<http://www.cnblogs.com/ggjucheng/archive/2012/01/14/2322659.html>

在kali终端下用wireshark打开pcap包，在显示规则里里输入tcp.port == 8090



导出对象--HTTP：





在保存的文件夹中查看找到一个tar压缩包，解压之后能发现一个png图片，里面就是KEY

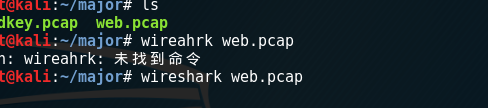
答案： KEY{Ss\_9F1k\_!}

第十一题：

知识点同第六题

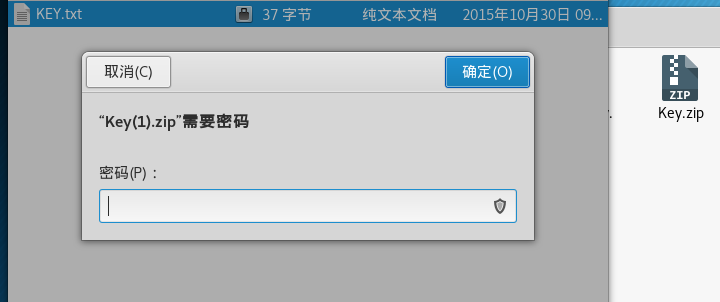
解题过程：

1. kali下wireshark下打开文件

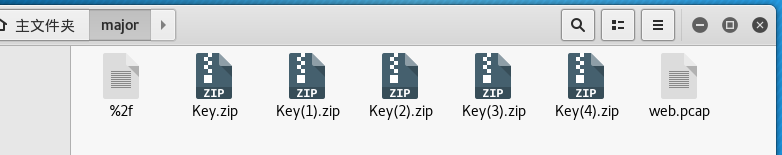


2．导出对象—http,解压文件夹

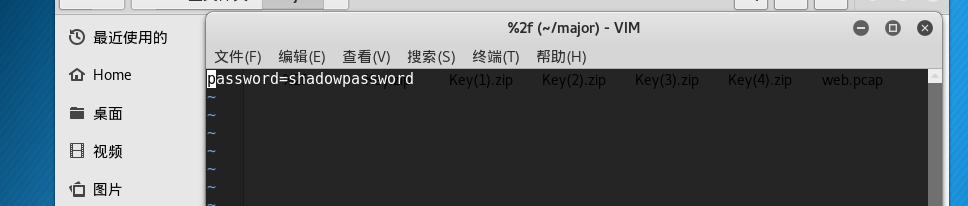




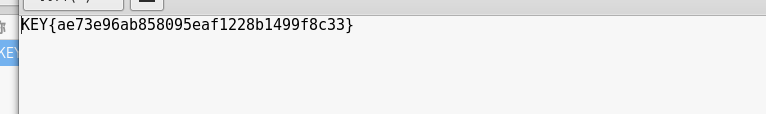
看到提示需要找出解压密码



发现有一个%2f文件，在终端用file命令查看文件类型，发现是一个txt文件，有vim编辑器打开文件侯发现密码



利用该密码打开压缩文件夹



找到答案。