**课程编号：A0802360040**

**信息安全工程实践3**

**实践报告**



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **姓名** | **黄能文** | **学号** | | **20184875** |
| **班级** | **软信1802** | **指导教师** | | **杨巍** |
| **开设学期** | **2020-2021春季学期** | | | |
| **开设时间** | **第1周——第2周** | | | |
| **报告日期** | **2021年3月21日** | | | |
| **评定成绩** |  | | **评定人** |  |
| **评定日期** |  |

**东北大学软件学院**

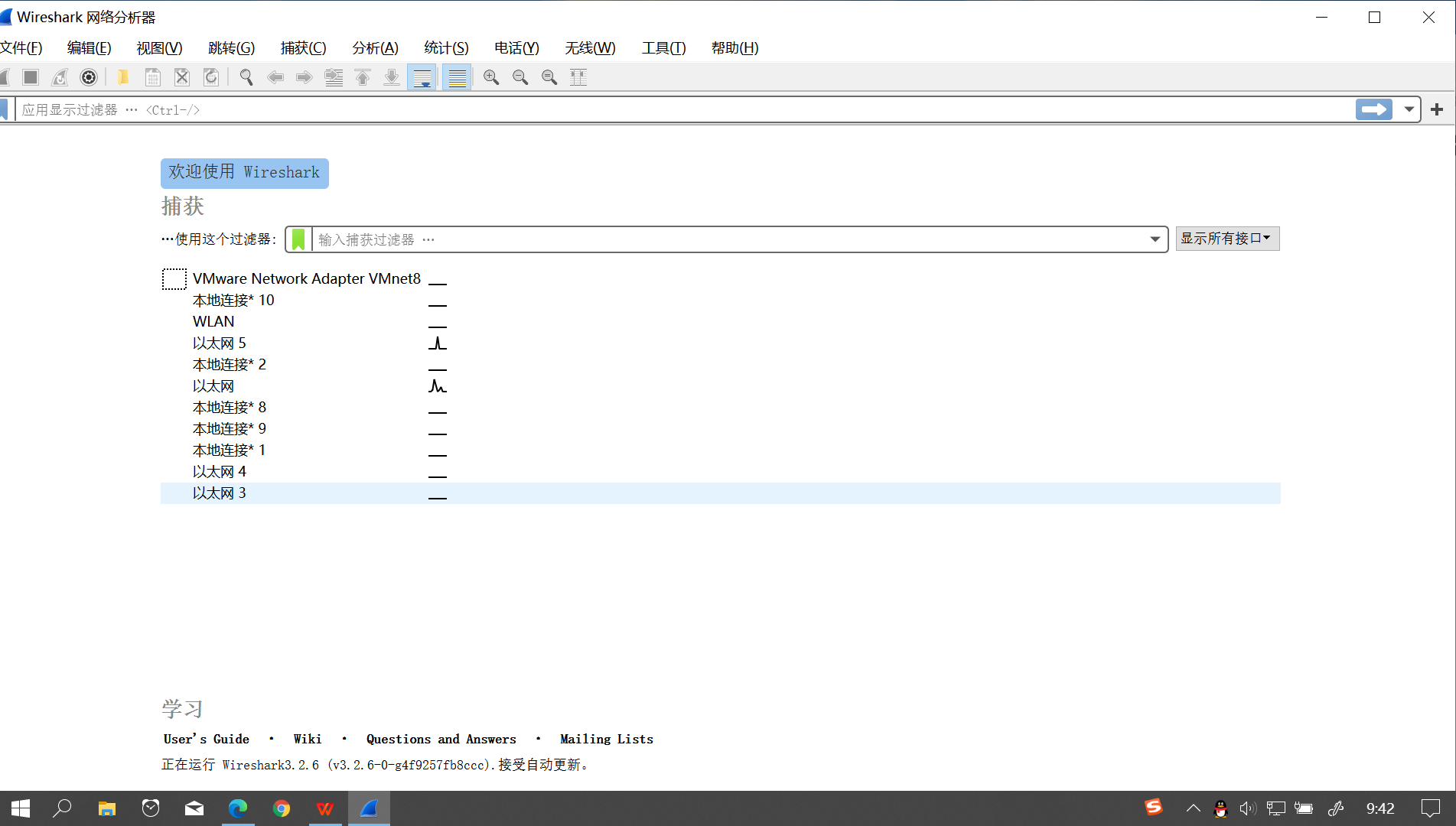
实验1 协议分析和网络嗅探

### 实践内容

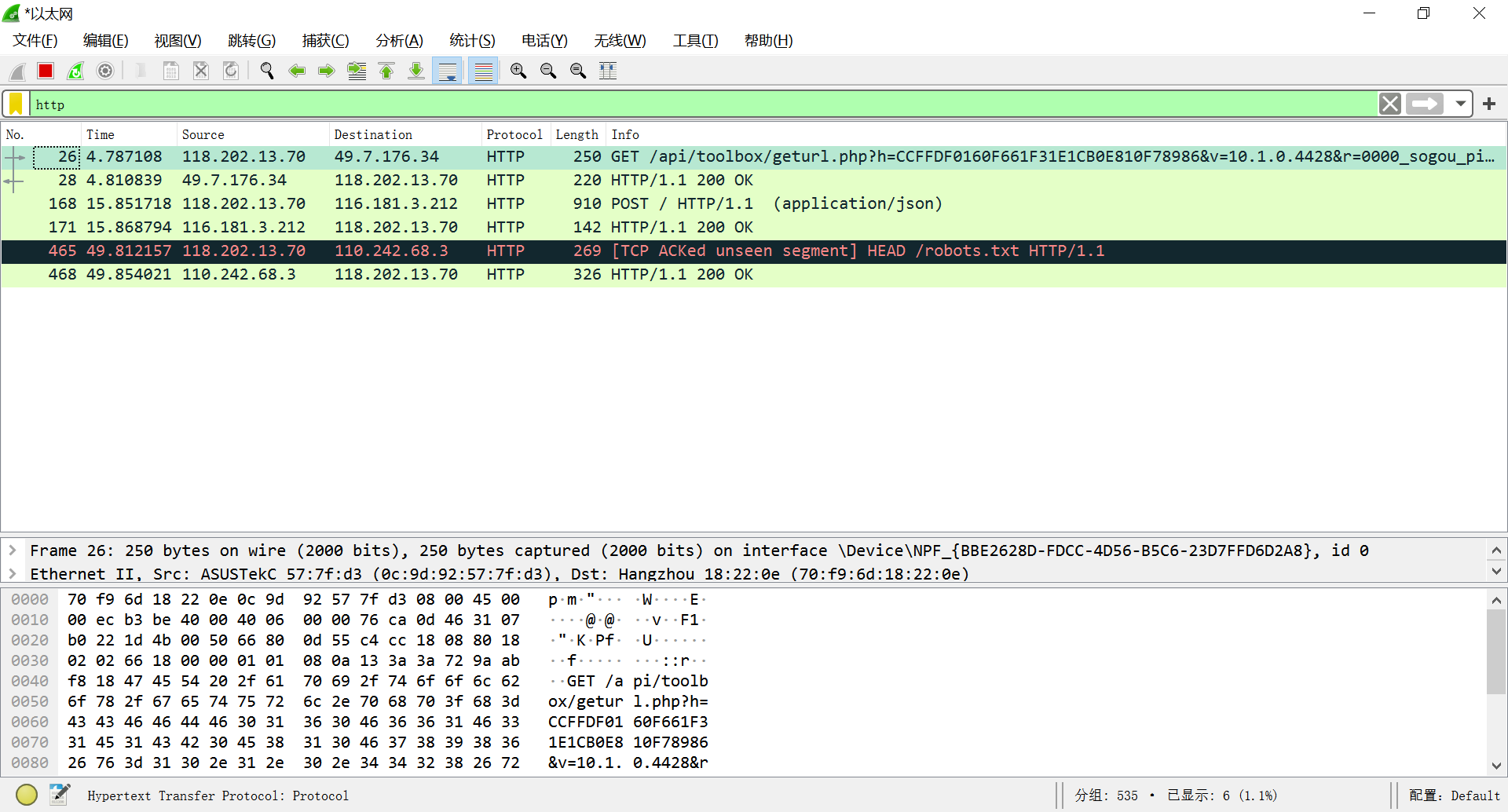
1. 通过使用Sniffer Pro 软件掌握Sniffer(嗅探)工具的使用方法，实现捕捉FTP、HTTP等协议的数据包；
2. 理解TCP/IP协议中多种协议的数据结构、会话连接建立和终止的过程；
3. 了解FTP、HTTP等协议明文传输特性，增强安全意识。

### 实践过程

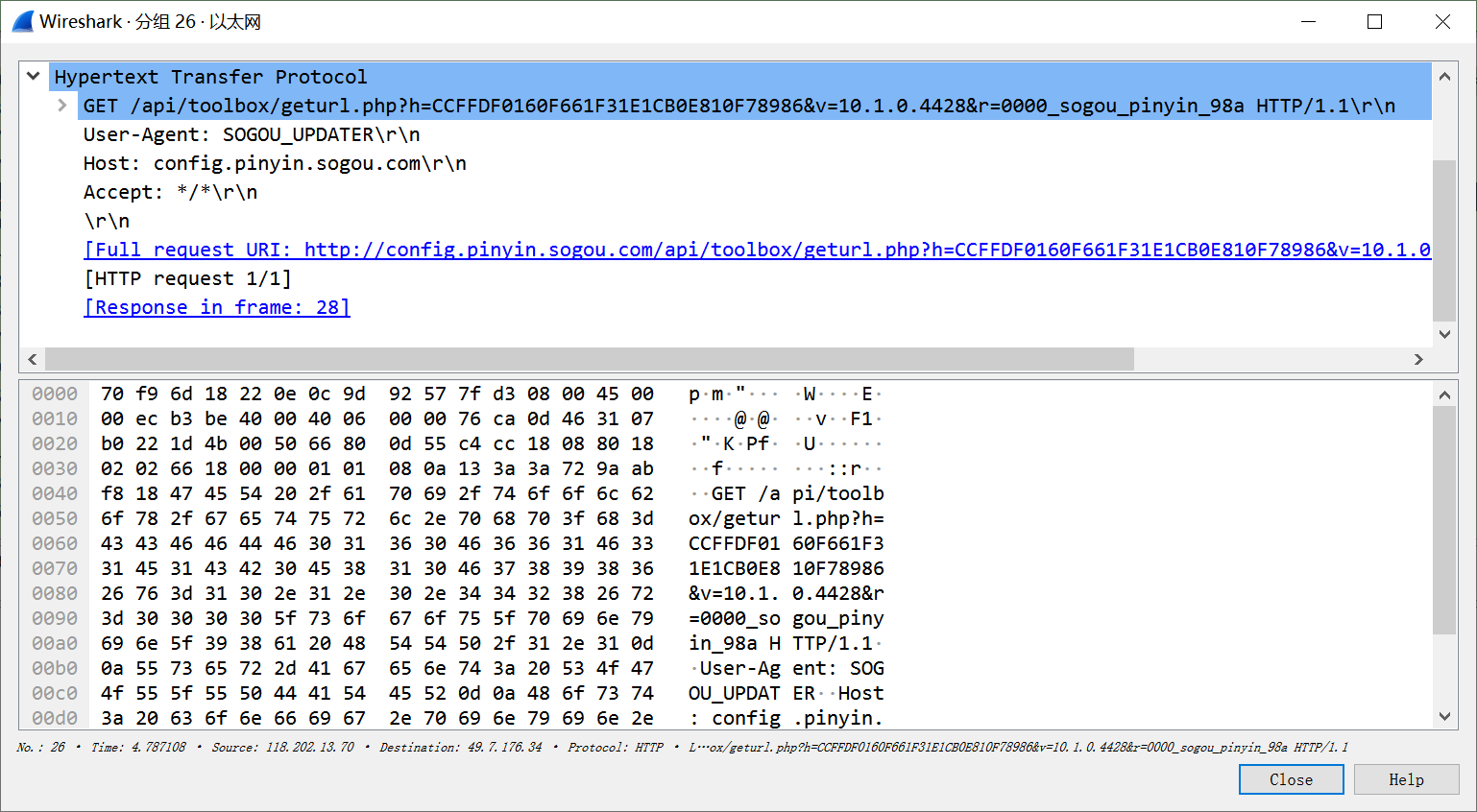
1.打开wireshark后，选择一个有数据包的网卡

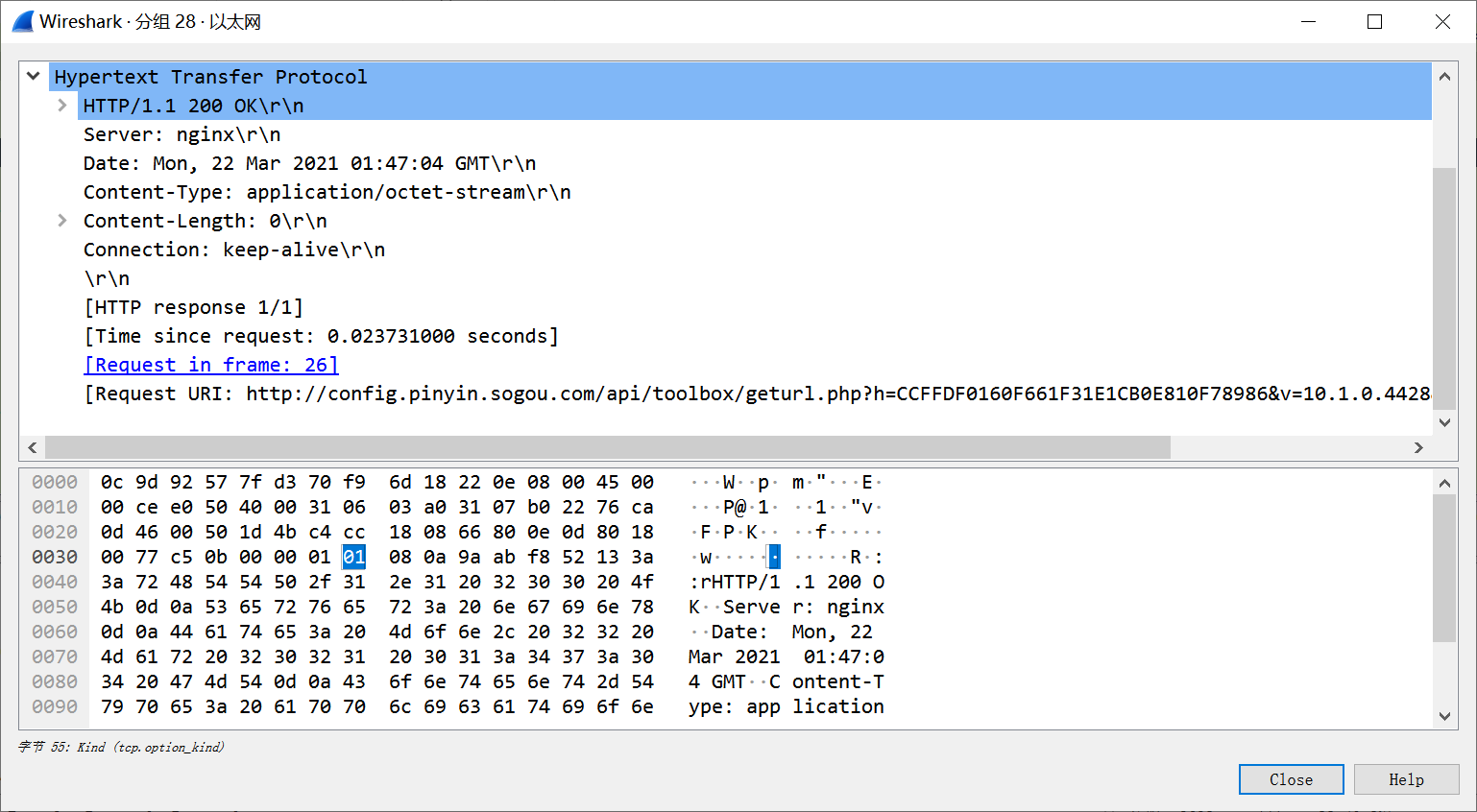


2.过滤器一栏中输入想要的数据包协议就能抓到。

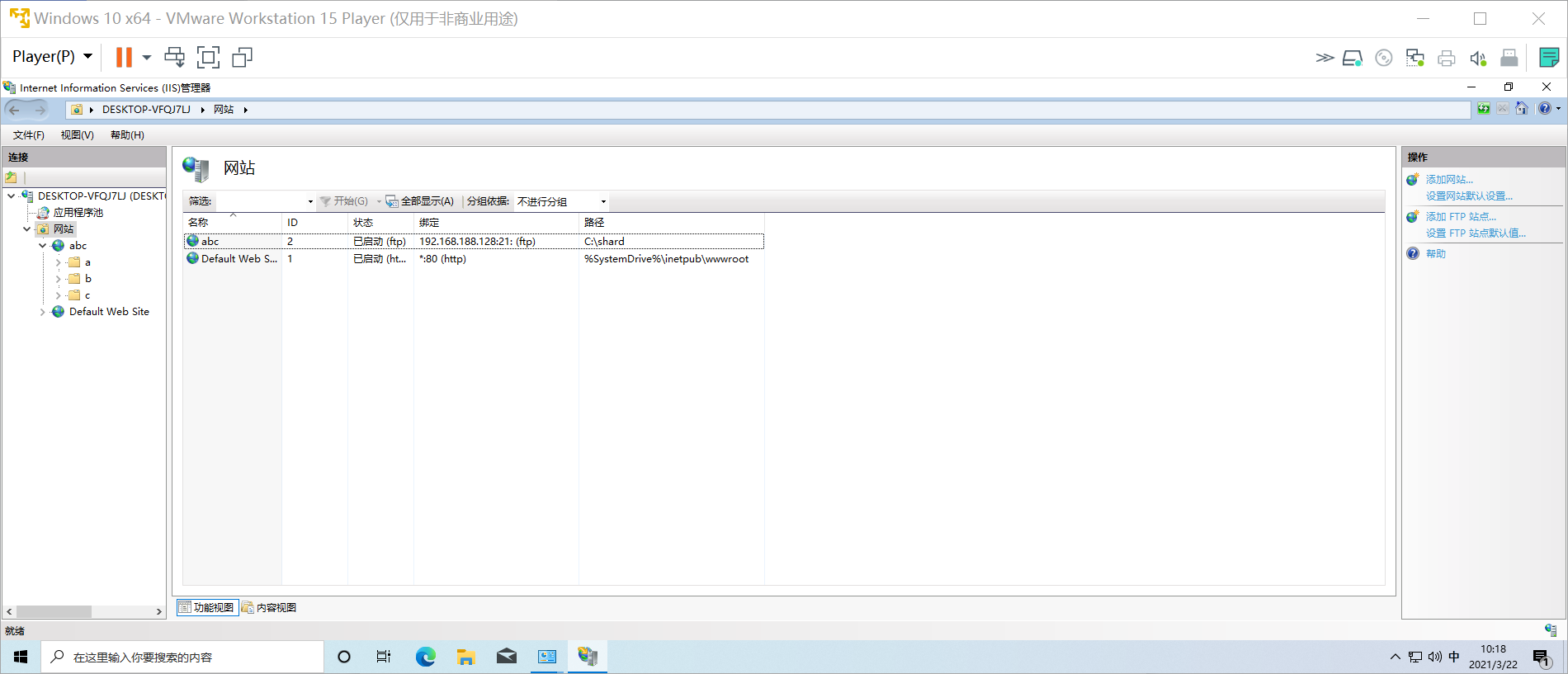


点击一个数据包就可查看详细信息，打开http数据包，查看http协议内容，发现是明文协议，请求包格式为：方法 内容 版本 换行 其它信息 换行 其它信息 等。响应包格式为：版本号，响应码及其他信息。

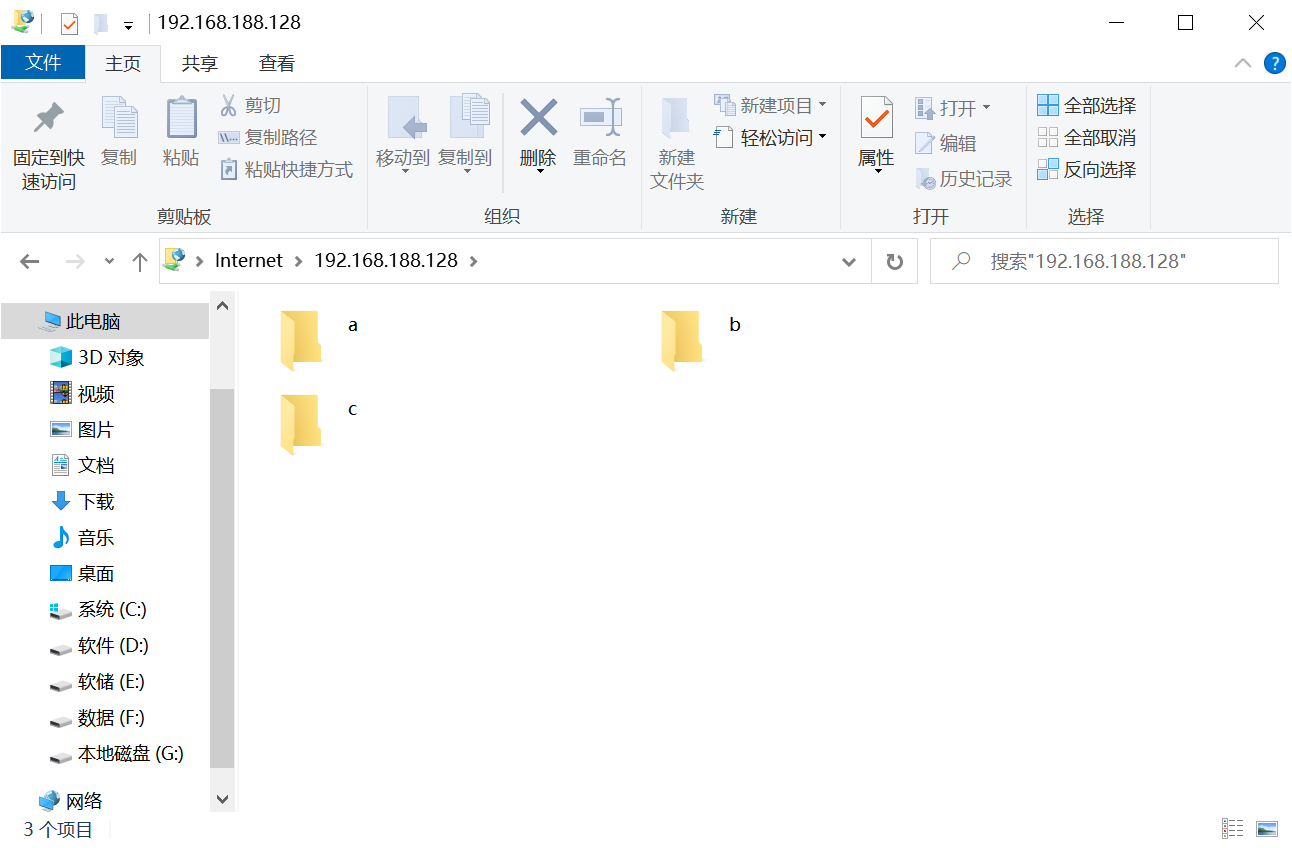




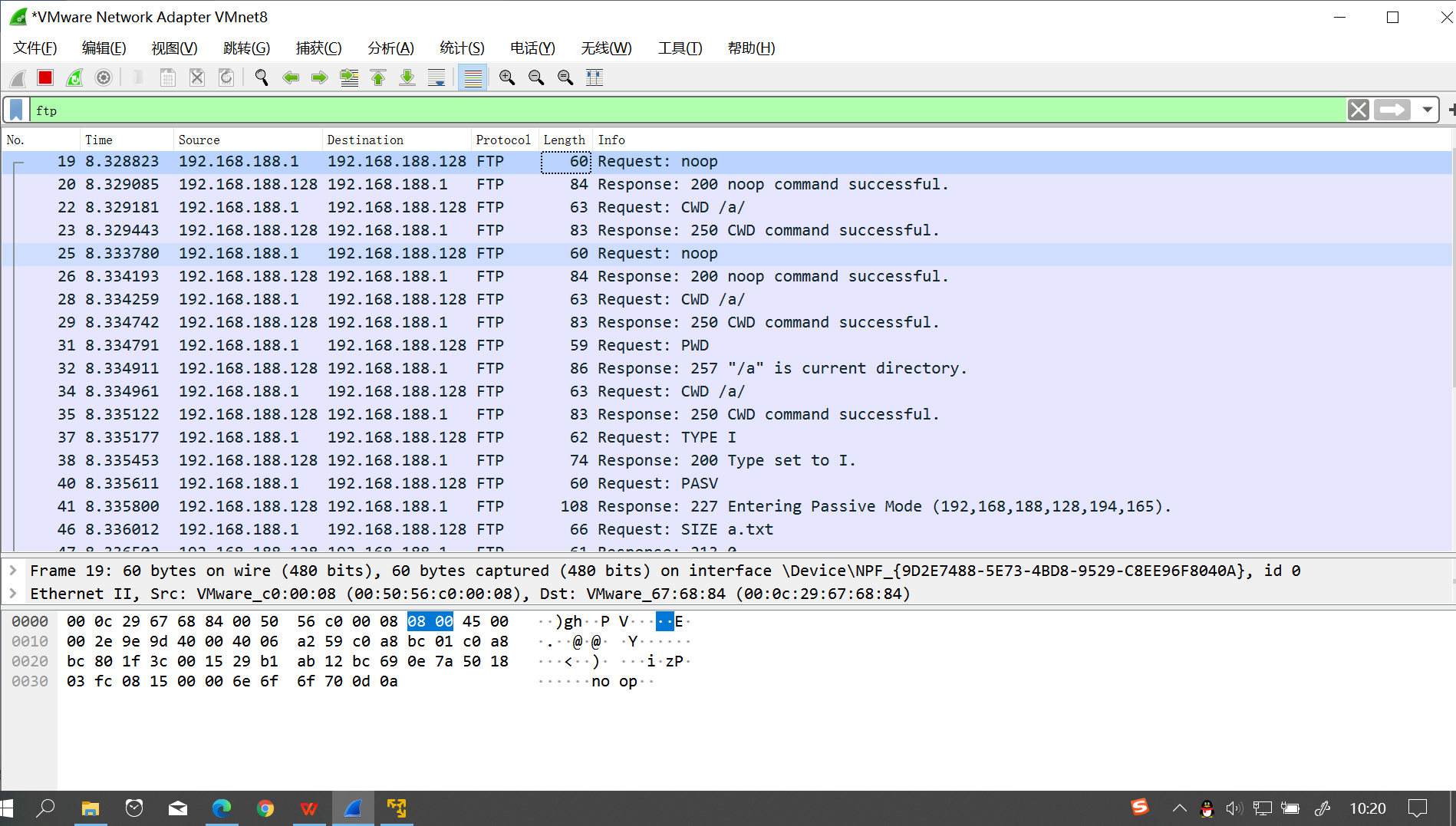
由于ftp数据包比较难找，根据网上的教程使用windows10自带的环境搭建ftp服务器，服务器如图：



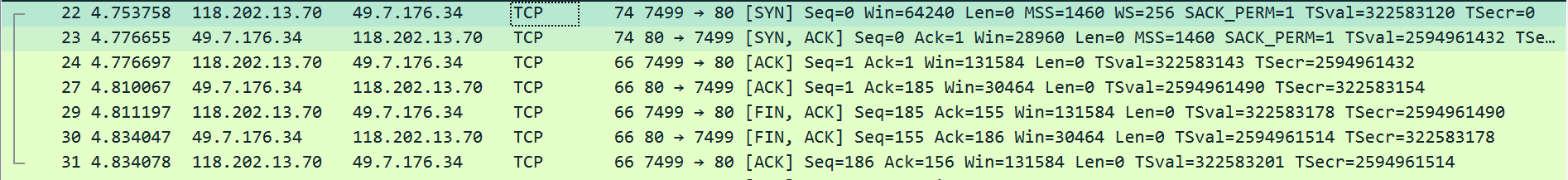
客户端使用资源管理工具即可，如图：



下载一个文件后就能抓到ftp数据包：



查看多个tcp数据包发现都有如下连接建立和断开格式，配合网上的资料分析，易知



标志位Syn是连接建立请求；syn，ack是连接确定响应；之后再跟一个ack数据包才算连接成功建立。Fin，ack表示断开和确定上一条信息，当双方都确定对方断开时就是断开连接了。

http和ftp协议使用明文传输，很容易被截获，需要额外加密才能保证安全，所以没证书的网站要慎用，没使用密码加密的更要小心。

实验2 ARP攻击的设计与实现

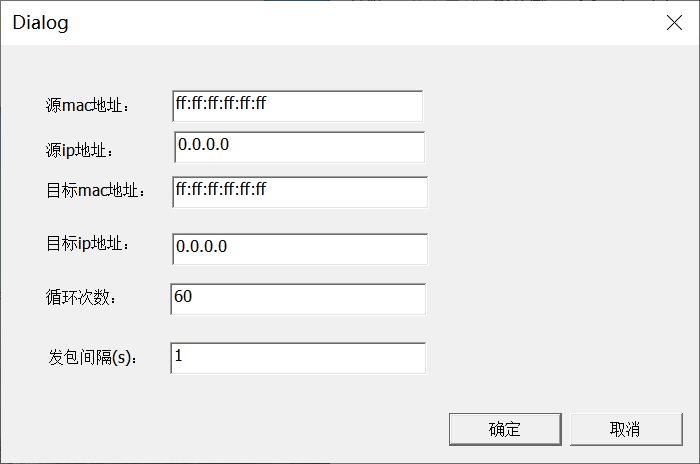
### 实践内容

1. 设计并实现ARP攻击
2. 可以设计并实现其他攻击

### 实践过程

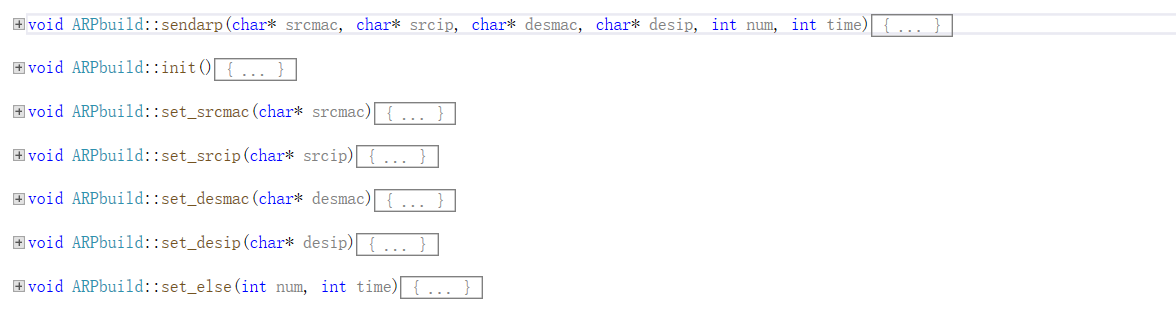
1. 设计一个软件，能修改其它主机的arp表中的网关，使该主机不能上网。
2. 应该提供目标主机mac，ip输入。伪造的自身主机的mac，ip输入。发包的个数，时间。

设计界面

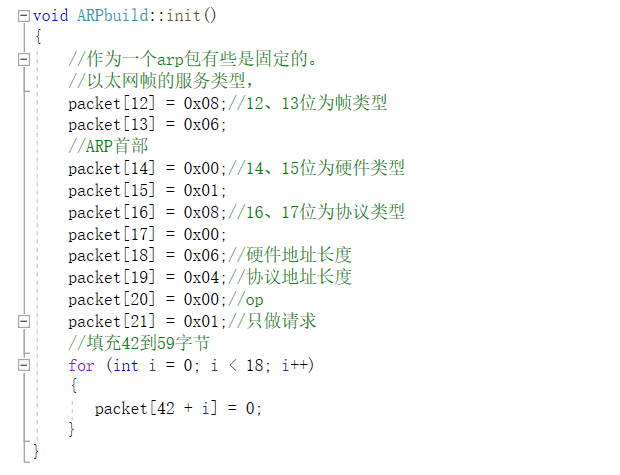


源ip地址填获得到的网关ip，源mac随便填。用虚拟机模拟受害者，发现arp表被改了，且上不了网。

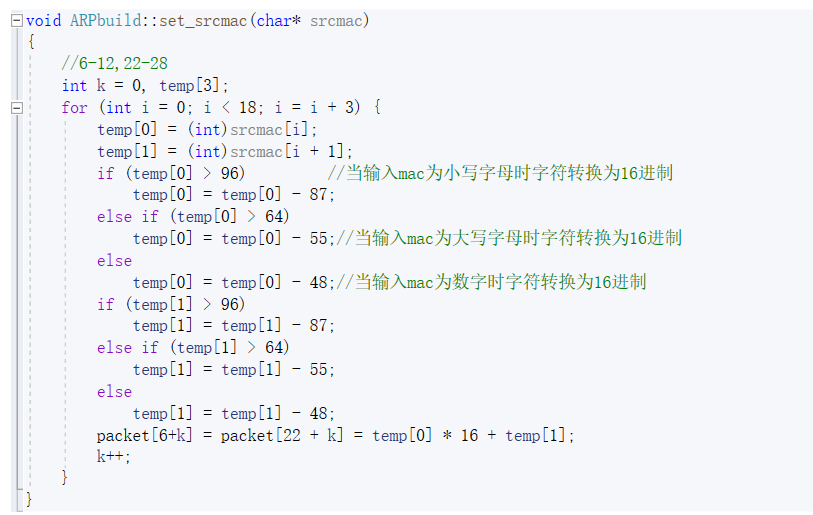
关键代码设计：对应各个输入栏的填充函数

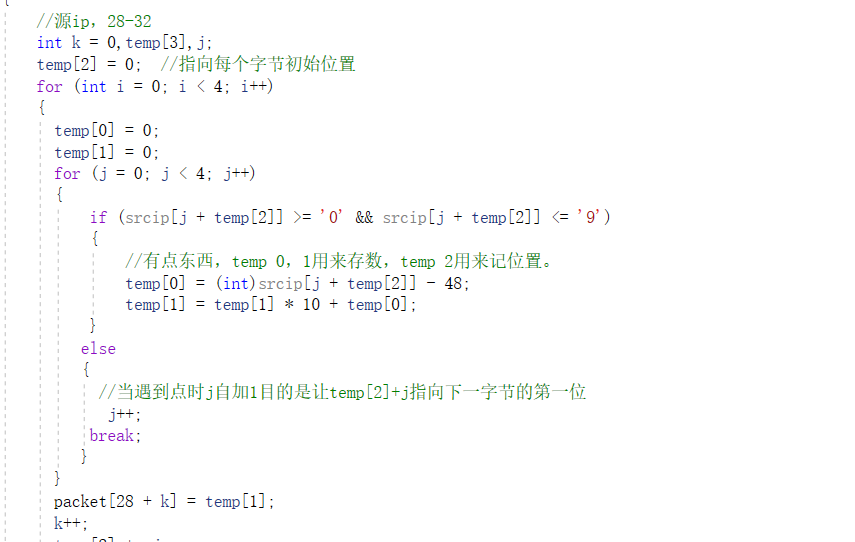


填充arp包中的固定数据



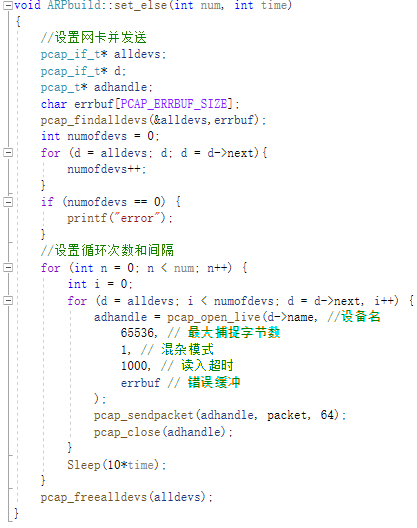
填充源mac





其它ip，mac输入类似

选择网卡发送：



实验3 新的网络攻击手段的论述

### 简介

### 攻击原理

### 工作过程或步骤流程（所用工具介绍）

### 功能或后果

### 防范手段与措施

### 结论（个人观点）

1.Air-fi无线信息窃取技术，即使是一个没有网络适配器的主机，也有可能发出无线信号传播信息，这种技术比较容易让人忽视，而导致重要信息泄露。

****2.其利用了任何电子设备都可在通电工作时产生电磁波的原理，最终达成了在相隔几米远的地方、以 100 bps 来泄露数据的速率。****攻击者可利用系统中的恶意代码，来操纵内存（DRAM）组件产生频率一致的电磁波。

1. 注入恶意代码，运行后能监听信息，并通过产生无线电泄密。
2. 重要信息泄露
3. 严格做好物理隔绝，要有着方面意识。
4. 类似air-fi这样的无线信号攻击还有很多，无线信号看不见，但一定不能放松警惕。

实践总结

1. 参考资料

https://www.ednchina.com/news/6149.html，Air-fi攻击相关资料

1. 实践总结

网络安全问题无处不在，还出其不意，需要每个安全人员共同维护。

评价表格：

|  |  |
| --- | --- |
| 考核标准 | 得分 |
| （1）实现实践要求基本内容（60%）； |  |
| （2）实验过程中，具有严谨的学习态度和认真、踏实、一丝不苟的科学作风（10%）； |  |
| （3）所做实验具有一定的创新性（20%）； |  |
| （4）实验报告规范（10%）。 |  |