第5章

网络取证实训

网络取证是指利用计算机网络技术，按照符合法律规范的方式，对网络事件进行可靠的分析和记录，并以此作为法律证据的过程。网络取证是打击网络犯罪的必要和不可或缺的技术。在过去的十年中，网络威胁的数量呈指数级增长，其中包括网络诈骗、网络欺凌、恐怖主义等各种犯罪行为。网络取证技术专家的责任是使用不同的网络取证工具来抓取、记录和分析网络事件以发现安全攻击或其他问题事件的来源。本章通过相关实验，让读者对网络取证涉及的相关知识与技术有所了解，掌握利用常见的网络取证工具来获取和分析网络证据。

5.1 网站远程证据固定

5.1.1 预备知识：Hosts 文件

Hosts 是一个没有扩展名的系统文件，可以用记事本等工具打开，其作用就是将一些常用的网址域名与其对应的 IP 地址建立一个关联“数据库”，当用户在浏览器中输入一个需要登录的网址时，系统会首先自动从 Hosts 文件中寻找对应的 IP 地址，一旦找到，系统会立即打开对应网页，如果没有找到，则系统会再将网址提交到 DNS 域名解析服务器进行 IP 地址的解析。也就是说 Hosts 里的配置优先级是高于 DNS 域名服务器的。

在 Windows 10 系统下，该文件在 C:\WINDOWS\System32\drivers\etc 目录中。Hosts 文件的作用为：①加快域名解析：对于要经常访问的网站，我们可以通过在 Hosts 中配置域名和 IP 的映射关系，提高域名解析速度。由于有了映射关系，当我们输入域名计算机时就能很快解析出 IP，而不用请求网络上的 DNS 域名服务器。②方便局域网用户：在同一个局域网里，建立 Hosts 里的 IP 映射，可以不用手动输入 IP，而是直接输入域名即可进行访问。③屏蔽网站：对于有些网站，我们不想访问，但总是自动弹出，可以利用 Hosts 把该网站的域名映射到错误的 IP 或本地计算机的 IP，这样就不用访问了。在 WINDOWS 系统中，约定 127.0.0.1 为本地计算机的 IP 地址，0.0.0.0 是错误的 IP 地址。

5.1.2 实验目的与条件

1. 实验目的

通过本实验，读者可了解网站远程证据固定的一般步骤，掌握关键步骤的操作要点，如

Hosts 文件检查、路由跟踪等，实验过程中特别注重流程上的合规性操作。

2. 实验条件

本实验所需要的软硬件清单如表 5-1 所示。

表 5-1 网站远程证据固定实验清单

序　　号	设　　备	数　　量	参　　数
1	取证工作站	1 台	Windows XP 以上
2	屏幕录像软件 (屏幕录像机(oCam))	1 个	500.0 绿色版
3	MD5.exe	1 个	绿色版

5.1.3 实验过程

步骤 1：运行屏幕录像软件，单击开始录制按钮，记录后续证据固定的所有操作过程。

步骤 2：打开 C：\WINDOWS\System32\drivers\etc 目录下的 Hosts 文件，检查确认目标网站没有在此做 IP 映射，如图 5-1 所示。

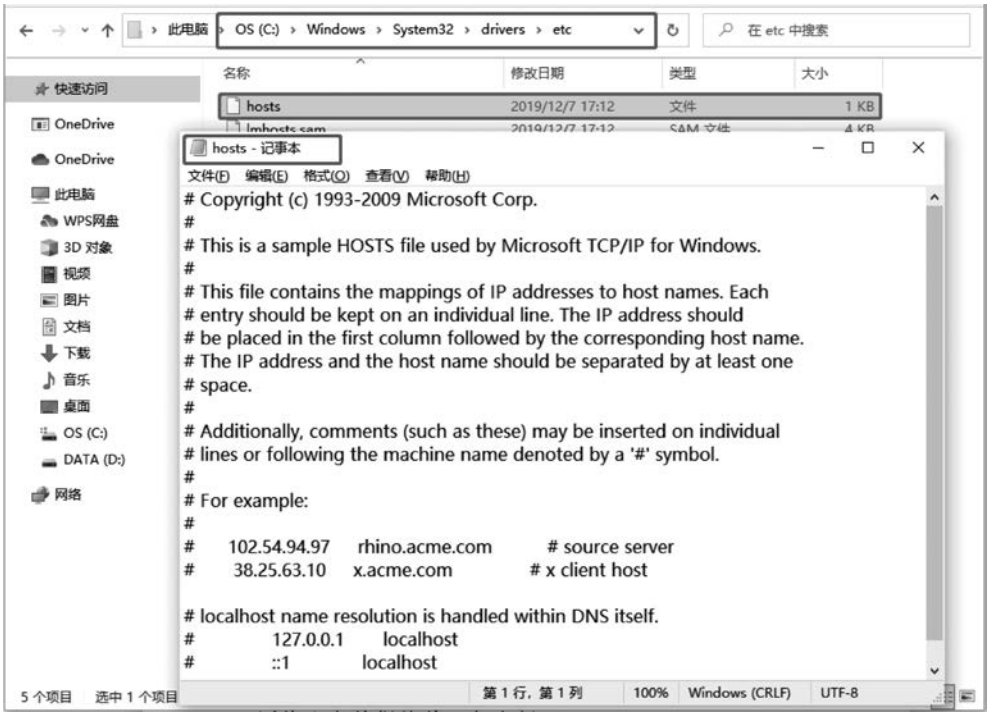

图 5-1 Hosts 文件

步骤 3：在网络和共享中心中，查看网络连接详细信息，注意检查本机网络连接设置与 DNS 设置(DNS 服务尽量调整为 114 等知名公共服务器)，如图 5-2 所示。

步骤 4：按住键盘“Win＋R”，输入“cmd”进入 DOS 命令符窗口。输入“ipconfig/flushdns”命令，按回车键，清除本地 DNS 缓存，如图 5-3 所示。

步骤 5：继续在 DOS 命令符窗口中输入“tracert”命令。检查目标网站路由跟踪路径，具体为：“tracert -w 500 -h 20 目标网站”，如图 5-4 所示。

图 5-2　网络连接详细信息

图 5-3　清除本地 DNS 缓存

图 5-4　路由跟踪目标网站

步骤 6：打开浏览器，清除浏览器所有历史记录，如图 5-5 所示。

步骤 7：打开国家授时中心(http://www.ntsc.ac.cn/)，校准本机时间，如图 5-6 所示。

步骤 8：访问工信部“ICP/IP 地址/域名信息备案管理系统”网站(beian.miit.gov.cn)，查询目标网站的备案信息，如图 5-7 所示。注意：输入的域名不要加“www”。

图 5-5　清除浏览器历史记录

图 5-6　国家授时中心标准时间

图 5-7　目标网站备案信息

步骤 9：在浏览器中访问目标网站，将首页完整截图；输入用户名密码登录网站，将用户后台完整截图；如有用户账号详情页，也需完整截图；根据案情需要，将其他需要固定的页面完整截图。

步骤 10：如果需要固定的证据包含网站上的视频文件，则打开查看网页源代码，找到视频标签，如图 5-8 所示。

图 5-8　网页源代码中视频元素

步骤 11：在该视频标签中的视频访问链接上单击鼠标右键，选择在新标签打开，即可在新页面中打开该视频。

步骤 12：在新打开的标签页中，单击视频右键属性，选择保存到本地磁盘即可，如图 5-9 所示。

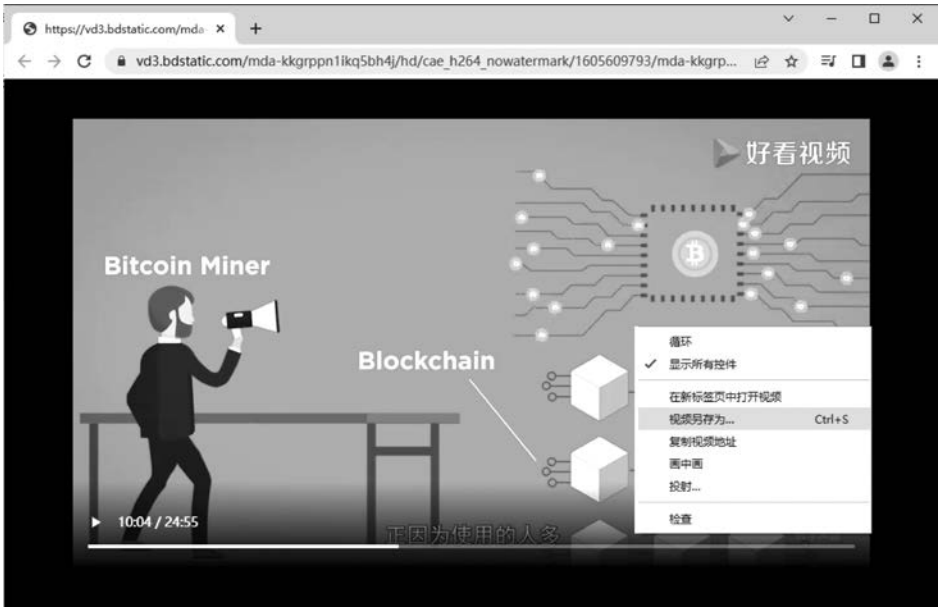

图 5-9　将视频保存到本地磁盘

步骤 13：将所有的截图与导出的视频均分别计算哈希值，并在 excel 表格中记录每个文件的详细信息，包括哈希值。

步骤 14：所有的导出数据打包成压缩文件，计算哈希值；所有的截图文件打包成压缩文件，计算哈希值。

步骤 15：结束录屏。

5.1.4 实验小结

公安机关在办理刑事案件过程中，特别是案件的初查阶段，运用网络远程勘验将网络空间中的涉案电子数据固定为证据，是广泛使用且不可或缺的电子数据取证措施。网络远程勘验的对象主要是远程计算机信息系统，区别于传统电子勘验，它没有实体检材，正因如此，网络远程勘验工作必须要形成规范化的流程、方法。经过十余年的积累，公安机关已逐步确立了网络远程勘验的专门规则和行业标准，但还须结合其特殊性和实际工作需要，对专门性、技术性问题进行实践探索。

在本实验中，值得注意的是，并不是所有网站的视频均可以直接找到链接并下载，src 属性不仅有非加密，也可以支持存放 blob 的加密源，此时无法直接获取视频的访问链接，而是需要通过进一步分析，如 M3u8 传输分片方案等，可借助一定的工具完成下载。

5.2 网络数据流分析

5.2.1 预备知识：流量分析

网络流量是指能够连接网络的设备在网络上所产生的数据流量。网络流量分析的主要方法如下：

① 软硬件流量统计分析。

基于软件的流量统计分析主要通过修改主机网络流入接口，使其具有捕获数据包的功能，常见的软件数据包捕获工具为 pCap(packet capture)。硬件主要有用于收藏和分析流量数据的设备方式，如流量镜像。

② 网络流量粒度分析。

在 bit 级上关注网络流量的数据特征，如网络线路传输速率、吞吐量变化等；在分组级主要关注 IP 分组到达的过程、延迟、丢包率；在流级的划分主要依据地址和应用协议，关注流的到达过程、到达间隔及其局部特征。

网络流量分析常用技术有：

① RMON 技术。

RMON(远程监控)是由 IETF 定义的一种远程监控标准，是对 SNMP 标准的扩展，它定义了标准功能以及远程监控和网管站之间的接口，实现对一个网段或整个网络的数据流量进行监控。

② SNMP 技术。

SNMP 技术基于 RMON 和 RMON Ⅱ，仅能对网络设备端口的整体流量进行分析，能获取设备端口的出入历史或实时的流量统计信息，但不能深入分析包类型、流向信息，具有实现简单、标准统一、接口开放的特点。

③ 实时抓包分析。

提供纤细的从物理层到应用层的数据分析。但该方法主要侧重于协议分析，而非用户流量访问统计和趋势分析，仅能在短时间内对流经接口的数据包进行分析，无法满足大流量、长期抓包和趋势分析的要求。

④ FLOW 技术。

当前 FLOW 的主流技术主要有两种，sFlow 和 NetFlow。

sFlow 是由 InMon、HP 和 Foundry Netfworks 在 2001 年联合开发的一种网络监控技术，它采用数据流随机采样技术，可以提供完整的、甚至全网络范围内的流量信息，能够提供超大网络流量（如大于 10Gbps）环境下的流量分析，用户能够实时、详细地分析网络传输过程中的传输性能、趋势和存在的问题。

NetFlow 是 Cisco 公司开发的技术，它既是一种交换技术，又是一种流量分析技术，同时也是业界主流的计费技术之一。它可以详细统计 IP 流量的时间、地点、使用协议、访问内容、具体流量。

流量分析是网络实时取证的重要内容，利用分析采集后的数据，对网络入侵时间、网络犯罪活动进行证据获取、保存和还原，流量分析能够真实、持续地捕获网络中发生的各种行为，能够完整地保存攻击者攻击过程中的数据，对保存的原始数据进行网络还原，重现入侵现场。

5.2.2　实验目的与条件

1. 实验目的

通过本实验，读者可以掌握以下内容：

（1）了解网络数据包分析软件 Wireshark 的使用方法；

（2）掌握网络数据流分析的一般过程和主要思路；

（3）案例背景：某公司内网网络被黑客渗透，简单了解后得知，黑客首先攻击了一台 web 服务器，破解了后台账户的密码，随之利用破解的密码登录了 mail 系统，获取了 vpn 的申请方式，然后登录了 vpn，在内网 pwn 掉了一台打印机。根据实验背景及素材，完成以下 10 道题目：

① 分析 A，黑客的 IP 地址是什么？

② 分析 A，被黑客攻击的 web 服务器，网卡 eth1 的 IP 地址是什么？

③ 分析 A，黑客扫描到的登录后台是什么？

④ 分析 A，黑客登录 web 后台使用的密码是什么？

⑤ 分析 A，网络账号“人事”所对应的登录密码是什么？

⑥ 分析 A，黑客上传的 webshell 文件是什么？

⑦ 分析 A，黑客找到的数据库密码是什么？

⑧ 分析 B，数据库的版本号为哪个？

⑨ 分析 B，“dou_config”表中，“name”列的值是“tel”的行中，“value”值是什么？

⑩ 分析 B，黑客破解了账号 ijnu@test.com 得到的密码是什么？

2. 实验条件

本实验所需要的软硬件清单如表 5-2 所示。

表 5-2　网络数据流分析实验清单

序　号	设　备	数　量	参　数
1	取证工作站	1 台	Windows XP 以上
2	Wireshark 软件	1 个	3.4.5
3	流量包 A.pcap	—	—
4	流量包 B.pcap	—	—

5.2.3 实验过程

步骤 1：分析实验题目，梳理解题思路，题目为黑客攻击类，一般会涉及到扫描器、webshell 等。

步骤 2：使用 Wireshark 软件打开流量包 A.pacp，首先要进行扫描器分析，常见扫描器特征有：WVS 扫描器通常默认情况下，会在请求的数据包中带有 wvs、acunetix_wvs_security_test、acunetix、acunetix_wvs 等字样；Nessus 扫描器默认情况下会包含 nessus 字样；APPscan 扫描器默认情况下会包含 APPscan 字样；绿盟极光扫描器一般会包含 nsfocus、Rsas 字样；sqlmap 扫描器大多情况下也会包含有 sqlmap 字样。

步骤 3：在 Wireshark 中设置过滤条件，过滤带有 wvs 的 http，如图 5-10 所示。由此可以判断出黑客的 IP 地址为 192.168.94.59，同时得到 web 服务器的 IP 地址为 192.168.32.189。

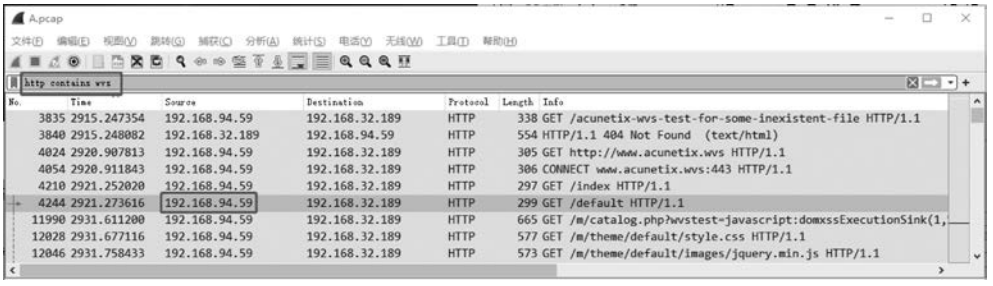

图 5-10 过滤“wvs”

步骤 4：分析 web 服务器 eth1 的 IP 地址，使用字符串搜索即可得到 eth1 的 IP 地址为 10.3.3.100。具体方法为：单击搜索按钮，选择搜索方式为“字符串”，在搜索栏输入“eth1”，单击“查找”按钮，即可得到 eth1 的 IP 地址，如图 5-11 所示。

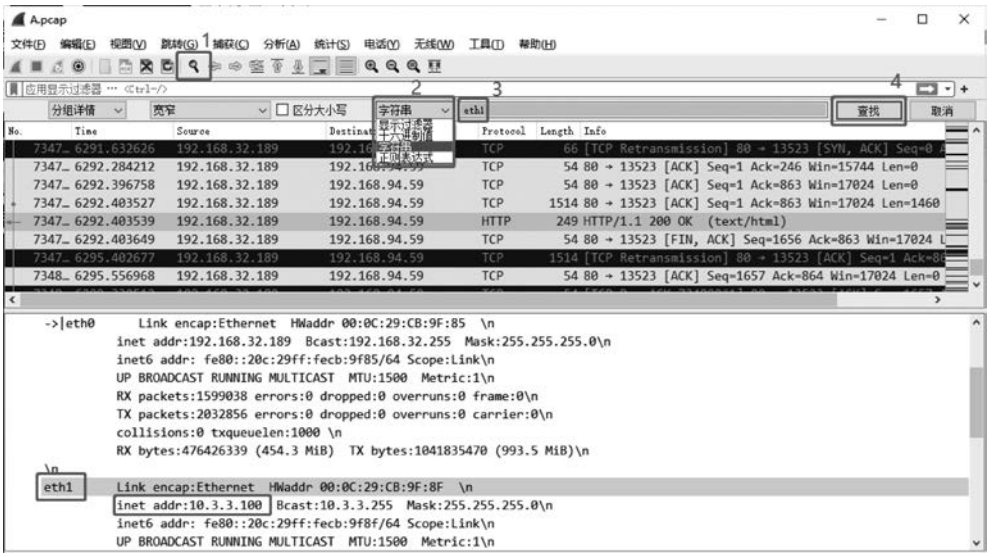

图 5-11 搜索 eth1 的 IP 地址

步骤 5：目前已经掌握了黑客 IP 地址及所使用的扫描器，通常网站后台的登录都包括 login、admin 等关键字，且登录后台 99% 使用的是 POST 方法。我们通过条件“http

contains login and ip. addr==192. 168. 94. 59 and http. request. method=="POST""进行过滤，可以得到登录后台是/admin/login. php，如图 5-12 所示。

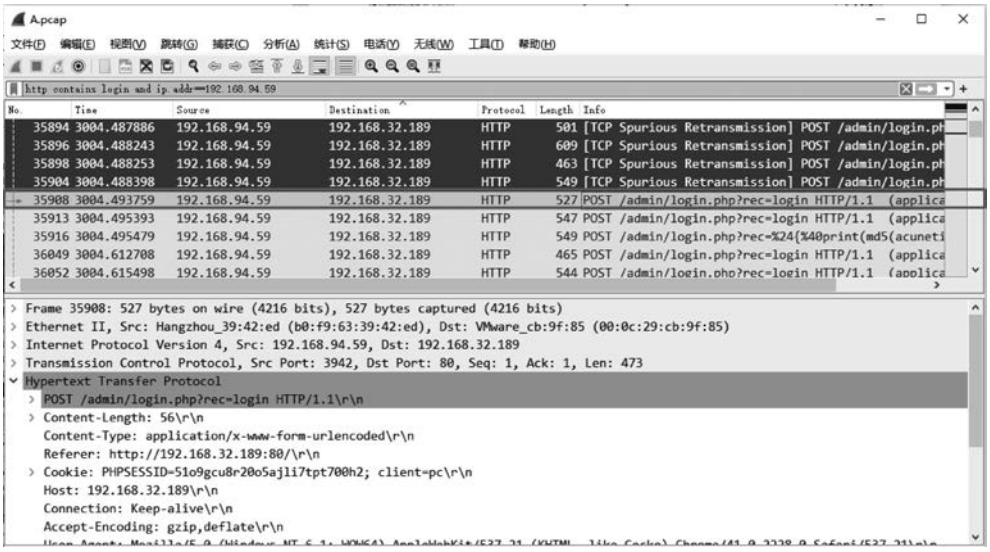

图 5-12　登录后台

步骤 6：查找黑客登录 web 后台使用的密码。通过上题过滤结果分析，从返回的字段长度可以推测，75x 的两个数据包存在问题，可能是登录成功。查看数据包内容即可得出密码是 admin!@#pass123，如图 5-13 所示。

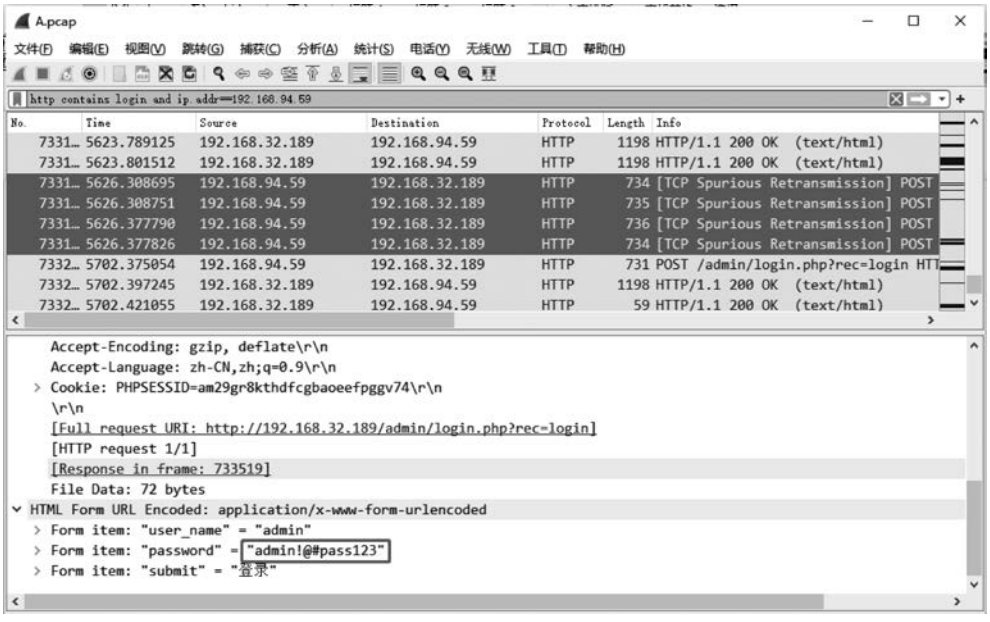

图 5-13　黑客登录密码

步骤 7：查看网站账号“人事”所对应的登录密码。通过对流量包 A 进行“http. request”过滤，得出密码为 hr123456，如图 5-14 所示。

步骤 8：查看黑客上传的 webshell 文件。通过以上分析已经确定了后台语言是 php，所

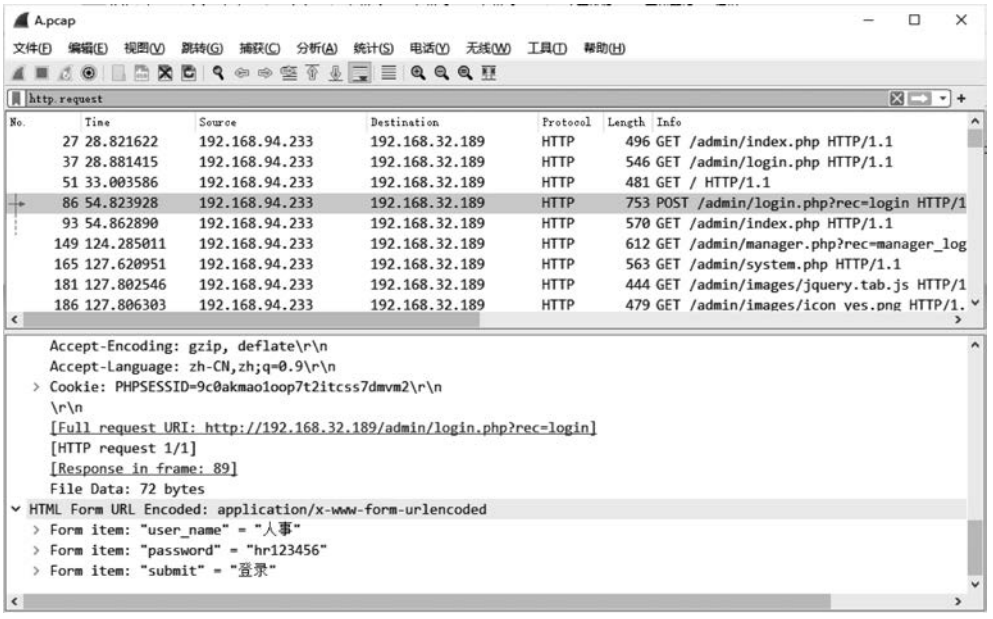

图 5-14 人事的登录密码

以只要找 eval 函数就可以。首先根据一句话木马的特征(eval 函数)先过滤一下数据包(ip.addr==192.168.94.59 and http contains eval and http.request.method =="POST"),得到 a.php 文件。通过对 a.php 文件分析,得出它就是 webshell 文件,且上传路径为"/images/article",如图 5-15 所示。

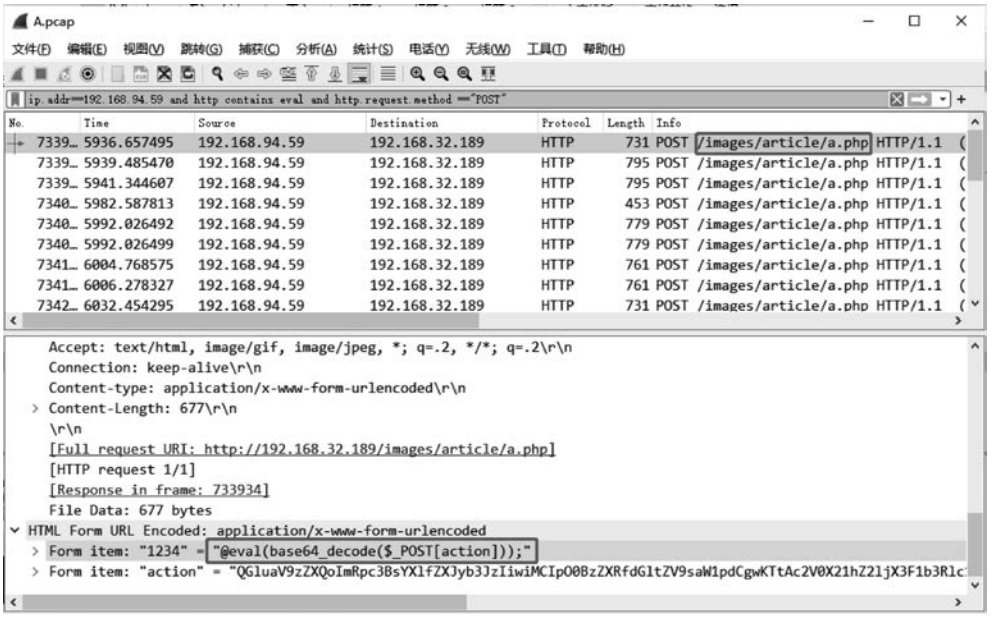

图 5-15 黑客上传的 webshell 文件

步骤 9:查看黑客找到的数据库密码。在 php 网站中,数据库配置文件通常为 config.php,database.php 等,通常通过过滤可以得出结果,此题中的 webshell 文件并未读取数据

库配置，我们可以查看返回状态码 200（数据库登录成功）进行过滤（ip. addr＝＝192. 168. 32. 189 and http. response. code＝＝200），从而得到数据库密码为 e667jUPvJjXHvEUv，如图 5-16 所示。

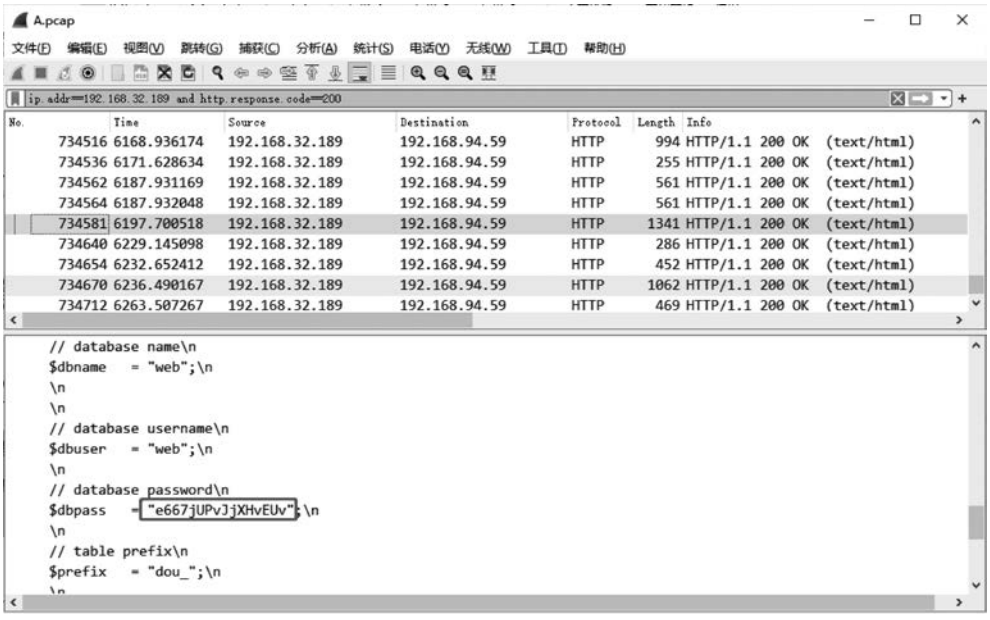

图 5-16　数据库密码

步骤 10：使用 Wireshark 软件打开流量包 B. pacp，过滤 mysql 协议，即可得到数据库版本号为 5. 5. 49，如图 5-17 所示。

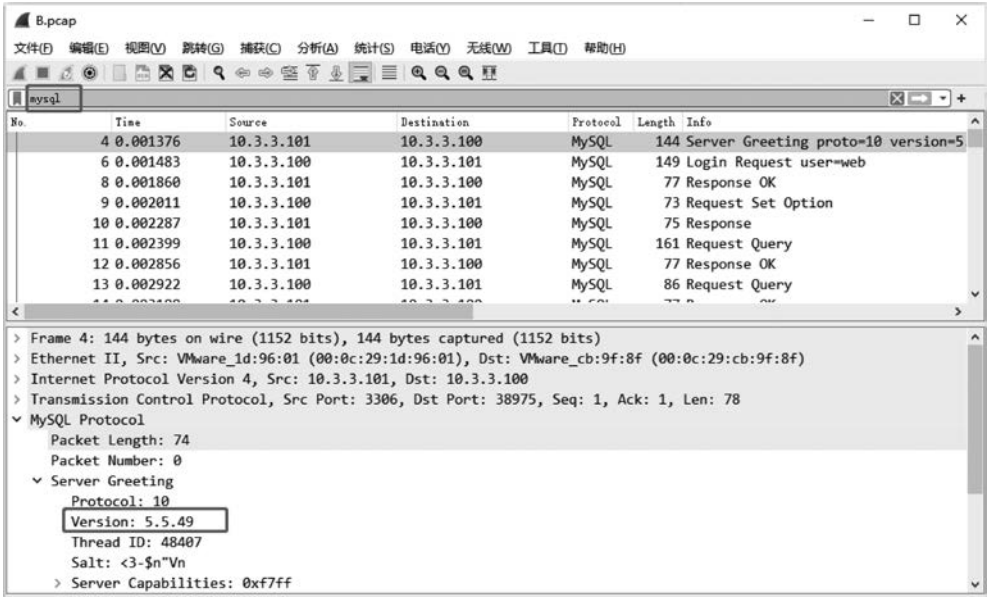

图 5-17　数据库版本

步骤 11：搜索关键字 tel，即可得到在“dou_config”表中，“name”列的值是在“tel”的行中，“value”值为 0596-888888，如图 5-18 所示。

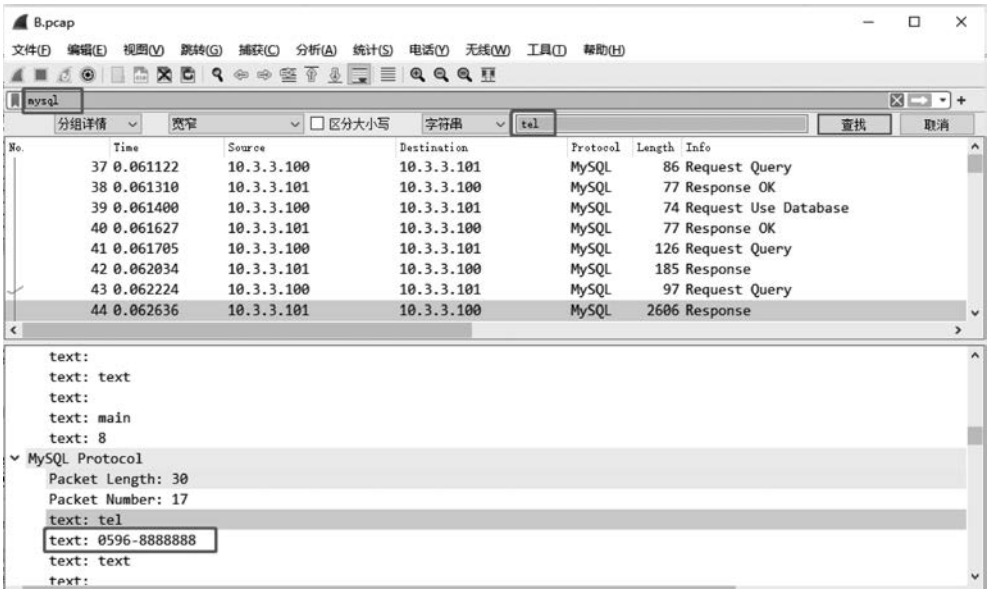

图 5-18 “tel”的行中的“value”值

步骤 12：使用以下的语法进行过滤：tcp contains "ijnu@test.com"，得到数据库密码为 b78f5aa6e1606f07def6e839121a22ec，如图 5-19 所示，该值为 MD5 值，解密为“edc123!@#”。

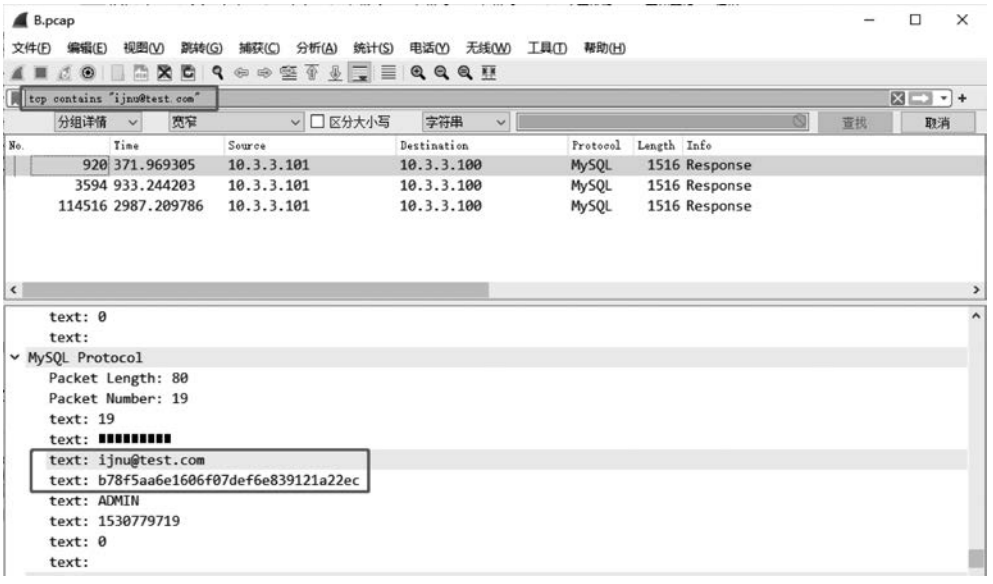

图 5-19 账号密码

本实验比较真实地还原了黑客的攻击过程。通过对题目的分析，发现还有 vpn 账号、vpn 服务器，以及攻击者使用的邮箱等信息，感兴趣的读者可以尝试进一步分析。

5.2.4 实验小结

网络取证需要监测网络环境信息与网络数据流，进行数据包的捕获与分析。网络环境的相关信息主要依靠 OSSIM 系统中的 IDS 等进行获取。这一系列的工具可以用来进行网

络信息收集与网络安全监测、IP/MAC 地址的分析与定位、TCP/UDP 端口与 DHCP 列表监测、SMTP 活动记录等。在进行网络包捕获方面，使用的技术包括基于 Libpcap 库、PF_RING 接口、直接使用系统调用等多种。

在被捕获的网络流中，网络包会按照它们在网络上传输的顺序显示，相关网络取证工具可以对这些包进行重组，即将这些包组织成两个网络连接点之间的传输层连接。虽然很多取证工具可以对未重组的原始数据进行分析，但是这样会造成非标准端口协议的丢失以及无法应对数据编码与加密传输干扰的问题。

网络取证中的相关性分析研究主要因为网络攻击行为往往是分布、多变的，因此对结果的认定需要将各个取证设施和取证手法得到的数据结合起来进行关联分析，以了解其中的相关性以及对结果产生的因果关系和相互确证，才可以重构过程。

5.3　Wireshark 解密 HTTPS 流量

5.3.1　预备知识：HTTP 与 HTTPS

HTTP(hyper text transfer protocol：超文本传输协议)是一种用于分布式、协作式和超媒体信息系统的应用层协议。简单来说就是一种发布和接收 HTML 页面的方法，被用于在 Web 浏览器和网站服务器之间传递信息。HTTP 默认工作在 TCP 协议 80 端口，用户访问 http://开头的网站都是标准 HTTP 服务。HTTP 协议以明文方式发送内容，不提供任何方式的数据加密，如果攻击者截取了 Web 浏览器和网站服务器之间的传输报文，就可以直接读懂其中的信息，因此，HTTP 协议不适合传输一些敏感信息，比如：信用卡号、密码等支付信息。

HTTPS(hypertext transfer protocol secure：超文本传输安全协议)是一种透过计算机网络进行安全通信的传输协议。HTTPS 经由 HTTP 进行通信，但利用 SSL/TLS 来加密数据包。开发 HTTPS 的主要目的是提供对网站服务器的身份认证，保护交换数据的隐私与完整性。HTTPS 默认工作在 TCP 协议 443 端口，它的工作流程一般为以下方式：

① TCP 三次同步握手；

② 客户端验证服务器数字证书；

③ DH 算法协商对称加密算法的密钥、哈希算法的密钥；

④ SSL 安全加密隧道协商完成；

⑤ 网页以加密的方式传输，用协商的对称加密算法和密钥加密，保证数据机密性；用协商的哈希算法进行数据完整性保护，保证数据不被篡改。

HTTP 与 HTTPS 的区别在于：

HTTP 明文传输，数据都是未加密的，安全性较差；HTTPS(SSL＋HTTP)数据传输过程是加密的，安全性较好。

使用 HTTPS 协议需要到 CA(Certificate Authority，数字证书认证机构)申请证书，一般免费证书较少，因而需要一定费用。证书颁发机构包括：Symantec、Comodo、GoDaddy 和 GlobalSign 等。

HTTP 页面响应速度比 HTTPS 快，主要是因为 HTTP 使用 TCP 三次握手建立连接，客户端和服务器需要交换 3 个包，而 HTTPS 除了 TCP 的三个包，还要加上 SSL 握手需要

的 9 个包，所以一共是 12 个包。

HTTP 和 HTTPS 使用的是完全不同的连接方式，用的 TCP 协议端口也不一样，前者是 80，后者是 443。

HTTPS 其实就是构建在 SSL/TLS 之上的 HTTP 协议，所以，HTTPS 比 HTTP 要更耗费服务器资源。

5.3.2 实验目的与条件

1. 实验目的

通过本实验，读者可以了解 HTTPS 流量的特点，掌握使用 Wireshark 解析 HTTPS 流量的一般过程。

2. 实验条件

本实验所需要的软硬件清单如表 5-3 所示。

表 5-3 Wireshark 解密 HTTPS 流量实验清单

序　号	设　备	数　量	参　数
1	取证工作站	1 台	Windows XP 以上
2	Wireshark 软件	1 个	3.4.5
3	流量包 Wireshark-tutorial-on-decrypting-HTTPS-SSL-TLS-traffic.pcap	—	—

5.3.3 实验过程

步骤 1：在 Wireshark 中打开“Wireshark-tutorial-on-decrypting-HTTPS-SSL-TLS-traffic.pcap”流量包。

步骤 2：使用 Web 筛选器过滤 Web 流量，包括 http/https 流量：(http.request or tls.handshake.type eq 1) and!(ssdp)，如图 5-20 所示。此 pcap 来自 Windows 10 主机上的 Dridex 恶意软件，所有 Web 流量(包括感染活动)都是 HTTPS 流量。没有密钥日志文件，看不到流量的任何详细信息，只有 IP 地址、TCP 端口和域名。

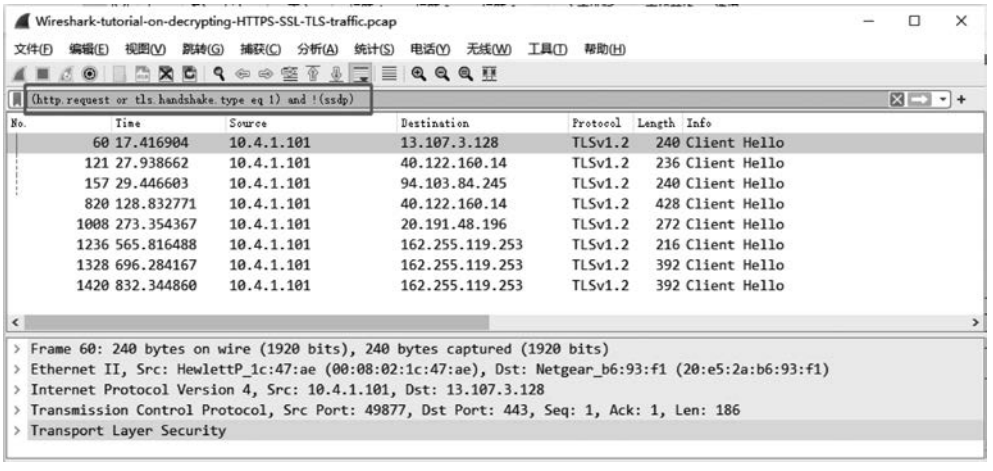

图 5-20 HTTPS 流量

步骤 3：单击菜单栏中的“编辑”按钮，选择“首选项”选项，打开“首选项”对话框，如图 5-21 所示。

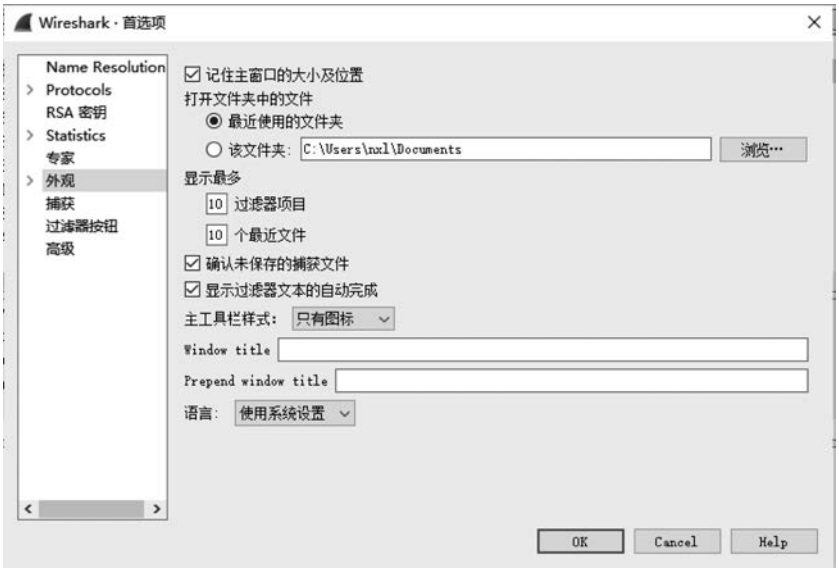

图 5-21　“首选项”对话框

步骤 4：在“首选项”对话框的左侧，单击 Protocols，选择 TLS，可以看到右侧“(Pre)-Master-Secret log filename”。单击“浏览”按钮，然后选择名为“Wireshark-tutorial-KeysLogFile.txt”的密钥日志文件，如图 5-22 所示。

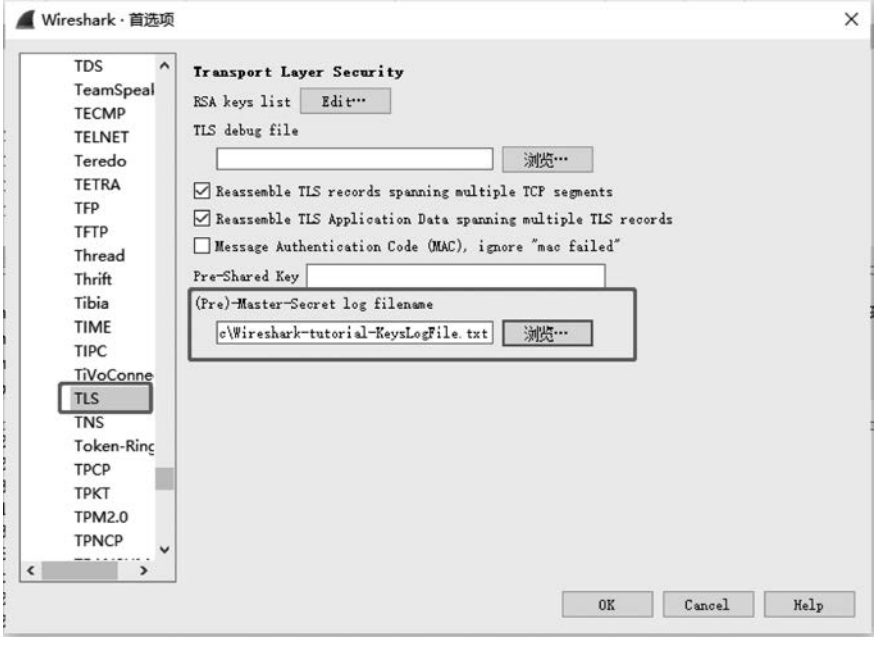

图 5-22　加载日志文件

步骤 5：单击 OK 按钮，Wireshark 会在每条 HTTPS 行下列出解密的 HTTP 请求，如图 5-23 所示。

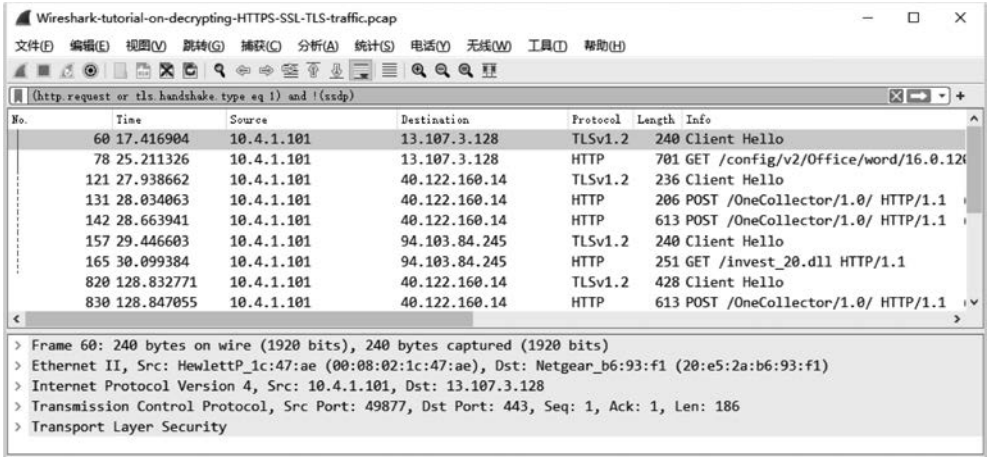

图 5-23 解密的 HTTP 请求

步骤 6：一一排查，在此 pcap 中可以看到隐藏在 HTTPS 通信中对 microsoft.com 和 skype.com 域的 HTTP 请求，还发现由 Dridex 发起的以下流量：①向 foodsgoodforliver.com 的 GET /invest_20.dll 请求，如图 5-24 所示；②向 105711.com 的 POST /docs.php 请求，如图 5-25 所示。

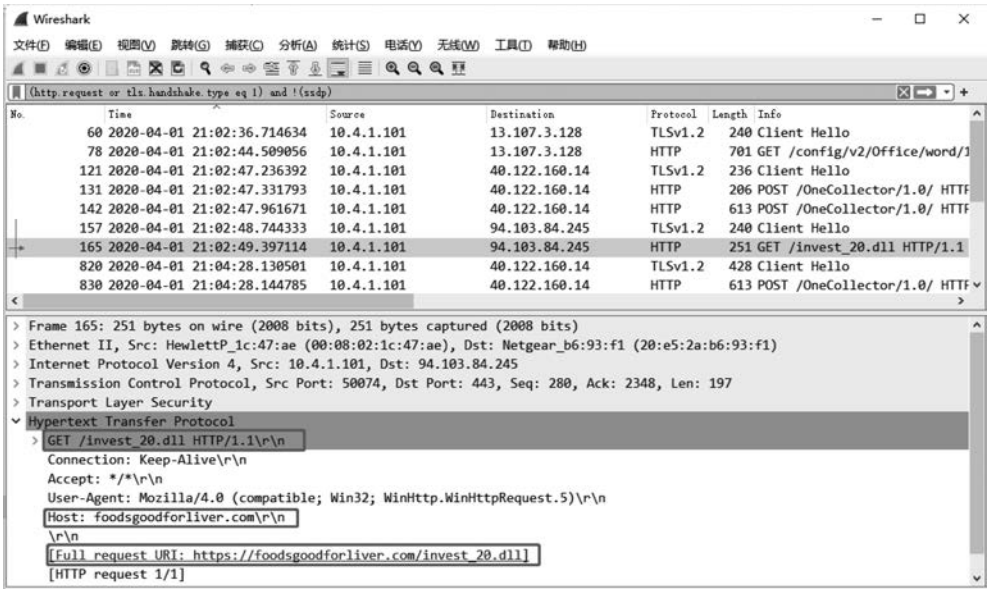

图 5-24 可疑流量 1

步骤 7：对 foodsgoodforliver.com 的 GET 请求返回了 Dridex 的 DLL 文件。对 105711.com 的 POST 请求是来自受 Dridex 感染的 Windows 主机的命令和控制(C2)通信。

追踪 foodsgoodforlive.com 的 HTTP GET 请求的 HTTP 流，如图 5-26 所示。

步骤 8：从 pcap 中导出此恶意软件，选择菜单栏中的“文件——导出对象——HTTP”，在弹出窗口中选择该 HTTP 对象，单击 save 按钮，如图 5-27 所示，即可将该 DLL 文件导出。

读者可自行尝试分析 105711.com 的 POST 请求的 HTTP 流，如图 5-28 所示。

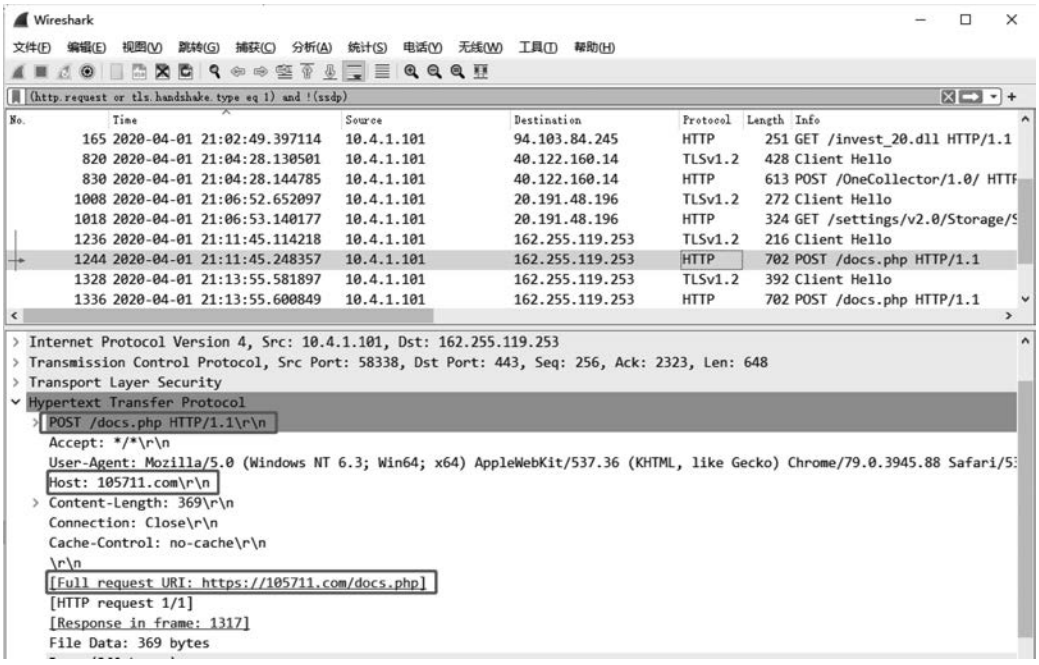

图 5-25　可疑流量 2

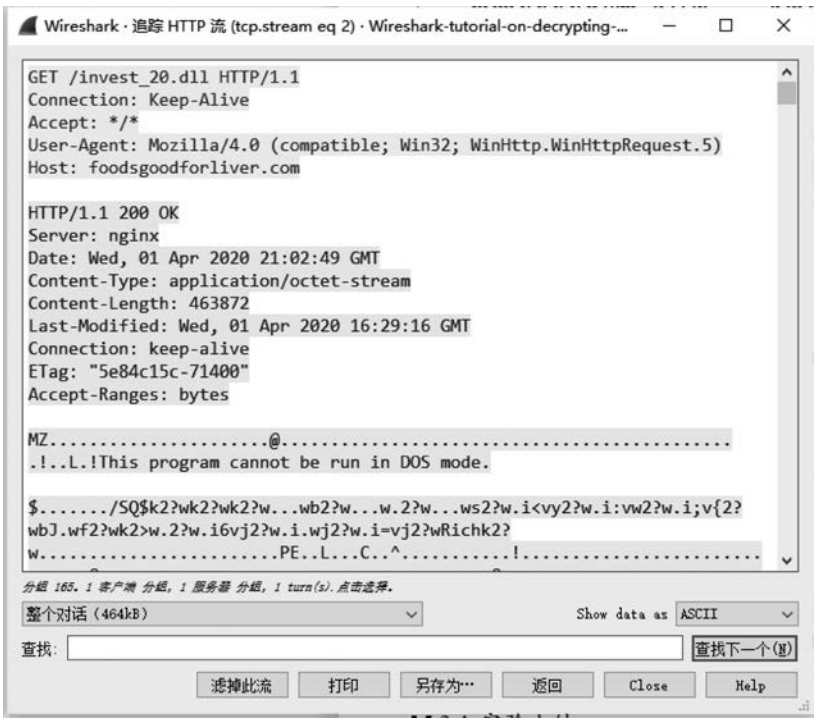

图 5-26　追踪 HTTP 流

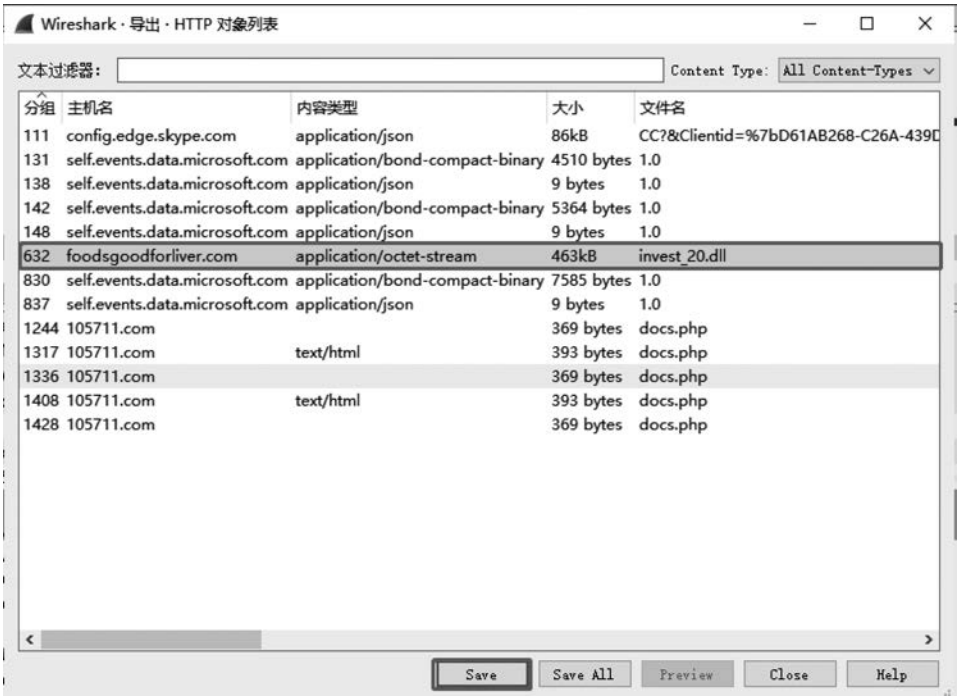

图 5-27 导出恶意软件

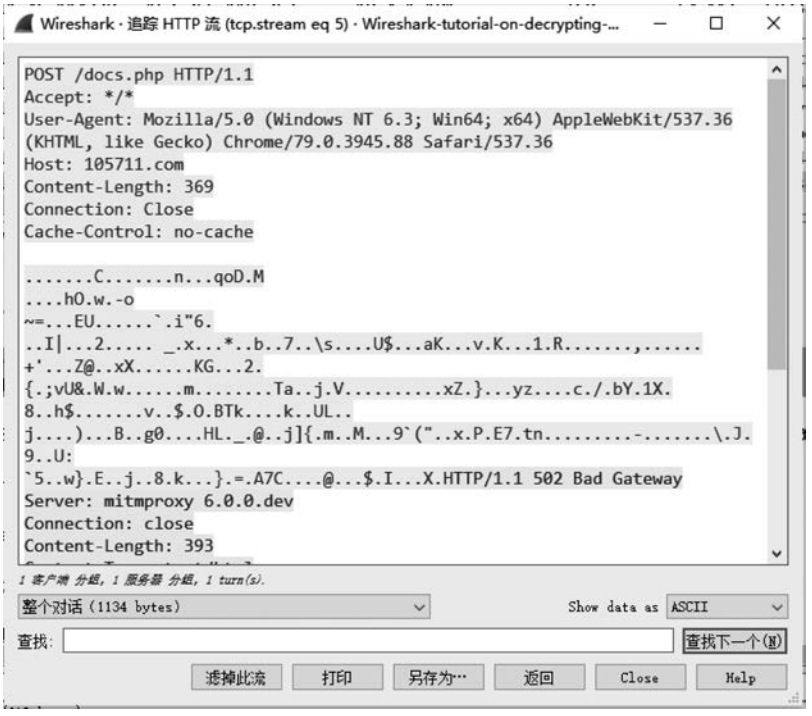

图 5-28 C2 流量

5.3.4 实验小结

在审查可疑网络活动时，经常遇到加密流量。大多数网站使用 HTTPS 协议，各种类型的恶意软件也使用 HTTPS，查看恶意软件产生的数据对于了解流量内容非常有帮助。

本实验使用 GitHub 上开源的 pcap 及其密钥日志文件作为实验素材，介绍了如何利用 Wireshark 从 pcap 中解密 HTTPS 流量。使用基于文本的日志解密方法，日志中包含最初记录 pcap 时捕获的加密密钥数据。最初记录 pcap 时，使用中间人(MitM)技术创建这些日志。如果在记录 pcap 时未创建任何此类文件，则无法解密该 pcap 中的 HTTPS 通信。