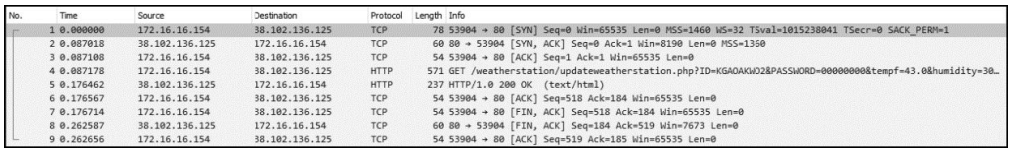
10.2.2 分析

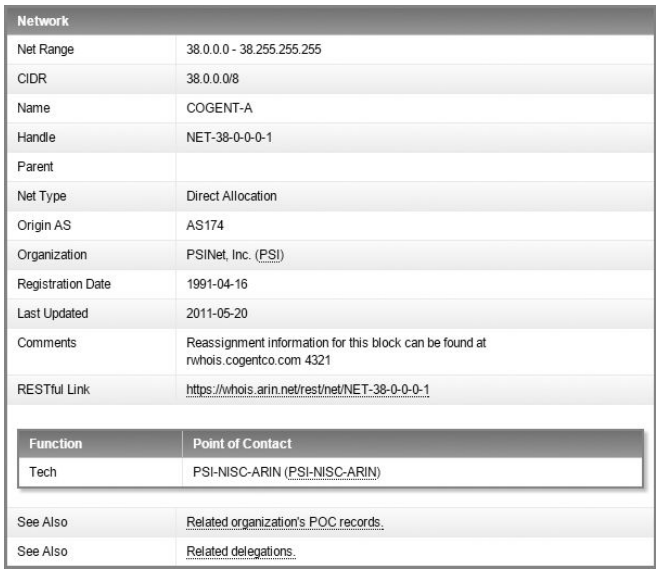
打开抓包文件后，你会看到，这又是一个 HTTP 通信的问题。抓取的数据包限定于 Pete 的本地气象数据接收器 172.16.16.154 与互联网上一个未知的远程设备 38.102.136.125 之间的单个会话中（见图 10-8）。



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.16.154	38.102.136.125	TCP	78	53904 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1015238041 TSecr=0 SACK_PERM=1
2	0.087018	38.102.136.125	172.16.16.154	TCP	60	80 → 53904 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1350
3	0.087100	172.16.16.154	38.102.136.125	TCP	54	53904 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
4	0.087178	172.16.16.154	38.102.136.125	HTTP	571	GET /weatherstation/updateweatherstation.php?ID=KGAOAKWO2&PASSWORD=00000000&tempf=43.0&humidity=30…
5	0.176462	38.102.136.125	172.16.16.154	HTTP	237	HTTP/1.0 200 OK (text/html)
6	0.176567	172.16.16.154	38.102.136.125	TCP	54	53904 → 80 [ACK] Seq=518 Ack=184 Win=65535 Len=0
7	0.176714	172.16.16.154	38.102.136.125	TCP	54	53904 → 80 [FIN, ACK] Seq=518 Ack=184 Win=65535 Len=0
8	0.262587	38.102.136.125	172.16.16.154	TCP	60	80 → 53904 [FIN, ACK] Seq=184 Ack=519 Win=7673 Len=0
9	0.262656	172.16.16.154	38.102.136.125	TCP	54	53904 → 80 [ACK] Seq=519 Ack=185 Win=65535 Len=0

图 10-8　分离出的气象站接收器通信

在检查这个会话的数据之前，让我们先来识别这个未知 IP。如果不进行进一步研究，我们将无法判断这个 IP 是否是 Pete 的气象站应该访问的地址，但是我们至少能够通过 WHOIS 查询来确定此 IP 是否是 Wunderground 服务器的一部分。你可以在大多数域名注册网站或区域互联网注册管理网站完成 WHOIS 查询。根据查询结果，这个 IP 看起来属于一家名为 Cogent 的互联网服务供应商（ISP）（见图 10-9）。结果中也提到了 PSINet 公司，但是搜索显示，21 世纪初 Cogent 获得了 PSINet 的大部分设备。



Network	
Net Range	38.0.0.0 - 38.255.255.255
CIDR	38.0.0.0/8
Name	COGENT-A
Handle	NET-38-0-0-0-1
Parent	
Net Type	Direct Allocation
Origin AS	AS174
Organization	PSINet, Inc. (PSI)
Registration Date	1991-04-16
Last Updated	2011-05-20
Comments	Reassignment information for this block can be found at rwhois.cogentco.com 4321
RESTful Link	https://whois.arin.net/rest/net/NET-38-0-0-0-1

Function	Point of Contact
Tech	PSI-NISC-ARIN (PSI-NISC-ARIN)

See Also	Related organization's POC records.
See Also	Related delegations.

图 10-9　WHOIS 数据识别出此 IP 的拥有者

在某些情况下，如果 IP 地址由一个组织或企业直接注册，那么 WHOIS 查询会返回组织名称。然而，多数情况下，公司不会自己去直接申请 IP，而是从因特网服务提供商（ISP）的 IP 池中获取地址。在这种情况下，另一种有效的措施是查找与 IP 地址相关联的自主系统编号（ASN）。组织需要申

请一个 ASN 用于在公网中支持某些路由方式。有很多方法可用于查找 IP-ASN 关联关系（一些 WHOIS 查询工具会自动查找 IP-ASN 关联），我推荐使用 Cymru 团队自动查询工具。使用这个工具查询 38.102.136.125，我们看到它与 AS 36347 相关联，此 ASN 属于「WUNDERGROUND – THE WEATHER CHANNEL, LLC, US」（见图 10-10）。这表明，至少，与气象站进行通信的设备属于期望中的组织。如果查询结果返回的组织信息与期望值不符，则说明 Pete 的接收器通信对象设备可能有误，但是在本例中并没有出现这种情况。

```
Executing commands. Please be patient!

v4.whois.cymru.com

The server returned 4 line(s).

[Querying v4.whois.cymru.com]
[v4.whois.cymru.com]
AS      | IP               | AS Name
36347   | 38.102.136.125   | WUNDERGROUND - THE WEATHER CHANNEL, LLC,US
```

图 10-10　对这个外网 IP 地址进行 IP-ASN 关联查询

确认了这个未知主机的所属组织信息后，我们将深入探讨通信的细节。这个会话相对较短：由一个 TCP 握手过程、一次 HTTP GET请求及响应和一个 TCP 断开过程组成。TCP 握手和断开似乎成功了，所以问题可能出现在 HTTP 请求中。我们跟踪 HTTP 请求的 TCP 流进行细致查看（见图 10-11）。

在 HTTP 通信过程中，首先由 Pete 的接收器向 WunderGround 发送一个GET请求。HTTP 内容部分没有数据，大量的数据通过 URL 进行传输 ❶。对于 Web 应用，通过 URL 查询字符串传输数据是很常见的，看起来，接收器使用这种机制更新天气信息。例如，你可以看到`tempf=43.0`、`dewptf=13.6`和`windchllf=43.0`这样的字段。WunderGround 信息收集服务器解析 URL 中的一些字段和参数，并将它们存储在数据库中。

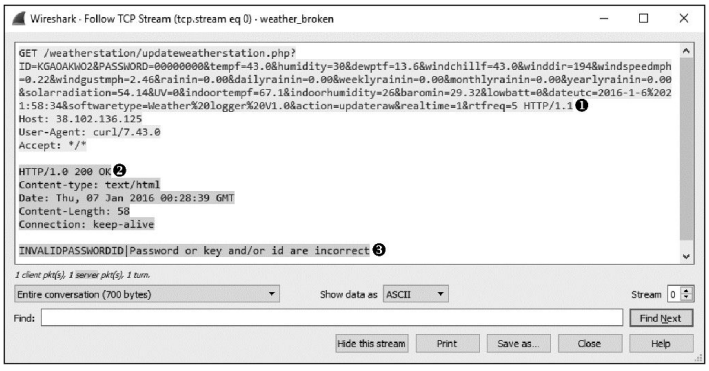


图 10-11　跟踪接收器通信的 TCP 流

根据第一印象，这个发往 WunderGround 服务器的GET请求似乎没有任何问题，但是对应的响应显示有一个错误。服务器的响应状态码为`HTTP/1.0 200 OK`❷，表明 GET 请求被成功接收，但是响应的消息体包

含了一条有用的信息，`INVALIDPASSWORD|Password or key add/or id are incorrect`❸。

回到请求 URL 部分，你会发现查询字符串的前两个参数为`ID`和`PASSWORD`。气象站使用这种方式完成在 WunderGround 服务器上的登录和验证。

本例中，Pete 的气象站 ID 正确，但是密码错误。由于某些未知原因，密码被置为 0。由于已知的最后一次通信成功发生在午夜，因此可能是一次升级或接收器重启，导致密码设置丢失。

> 注意
>
> 由于很多开发者选择使用 URL 传递参数，因此我们建议一般情况下不要如本例所示，将密码写在 URL 参数中。因为在不使用加密措施，如 HTTPS，的情况下，HTTP 通信将使用明文传输请求的 URL。所以，在使用 URL 参数传递密码时，碰巧正在监听通信链路的恶意用户能够截获你的密码。

此刻，Pete 接入他的接收器，输入新的密码。稍后，他的气象站重新开始同步数据。一个成功的气象站通信数据在 weather_working.pcapng 中。通信流如图 10-12 所示。

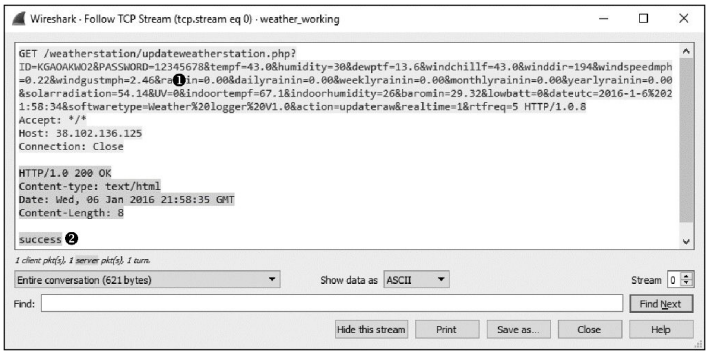


图 10-12　成功的气象站通信

现在，密码正确 ❶，WunderGround 服务器在应答的 HTTP 响应体中返回了一条success消息 ❷。