本文作者：creturn

起因：

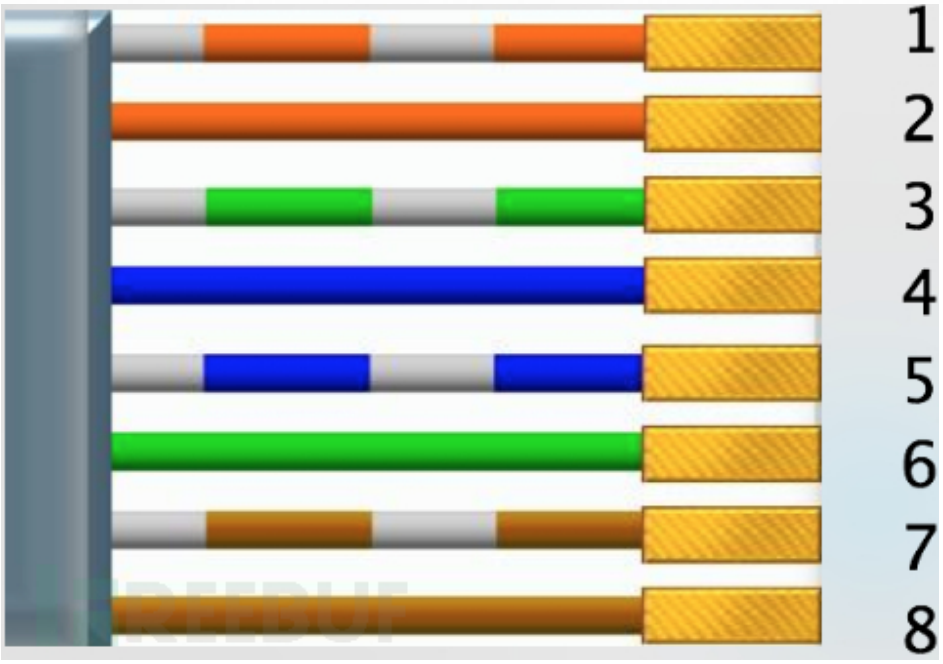
WEB “汪” 周末在家写着破PHP代码着实无聊，想着玩点有意思的东西，之前有看到 Throwing Star LAN Tap 不过一只没时间玩，兴致冲冲的打开某宝准备弄一个回来，一搜就傻眼了，一个1、2百块钱。作为屌丝买条裤子都觉得100块有点多怎么会花着钱。看着挺简单的决定自己动手弄一个。

分析：

先看看我们的分析对象

1. RJ45 接口网线

标准RJ45接口一共8根引脚，每根引脚的定义不一样，这里我们参考在100M工作下的引脚定义。看下图：



在这里得说明一下，标准RJ45接口是固定的但是，接线方式的标准常用有两种：T568B和T568A 。

市面上最常见的应该是T568B，上图就是T568B。 不管是哪种接线方式接口都是固定的引次不管那种接线方式在接下来分析的文章内容中都事宜。

T568B接口说明（百兆网络情况）：

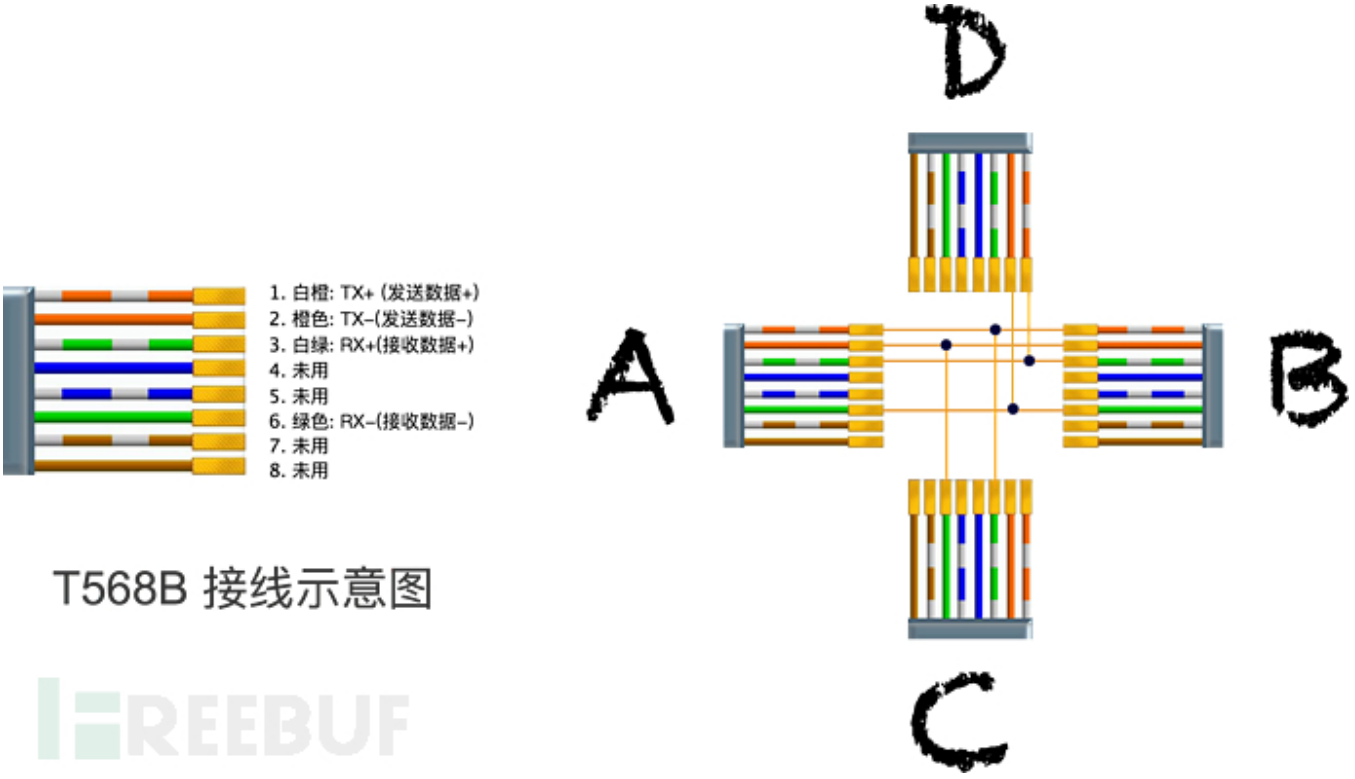
1. 白橙： TX+ （数据的发送＋）接口
2. 橙色： TX- （数据的发送－）接口
3. 白绿： RX+ （数据的接收+ ）接口

4. 蓝色： 未启用
5. 白蓝： 未启用
6. 绿色： RX- （数据接收－ ）接口
7. 白棕： 未启用
8. 棕色： 未启用

从说明中可以看到日常生活中所用的百兆网络只用到了4根线两根发送两根接收

2. 如何捕获数据

那么问题来了知道了接线的定义，那么我们如何才能捕获数据呢？其实中标题中就能看出来，木有错就是 “TAP” 也就是常见的搭线攻击。那么如何搭线才能正常的拿到数据呢？ 我画了个简单的图：



T568B 接线示意图

左边是T568B的说明图，可以看作是水晶头接触点朝上的平面图。

右边就是我们的重点搭线图：

A、B：A端和B端直接连接被搭线的两个网线接口。

C：C端这里可以看到是搭A、B通讯线上面的 1、2 根线（3、6 –> 1、2）也就是C端的数据接收接口搭线到A、B通讯线上面的发送数据接口。

D：D端这里接道的根C端相反搭A、B通讯的 3、6（1、2 –> 3、6）也就是D端的数据发送端搭线到A、B通讯线上面的数据接收端

其实细心的人已经发现，为啥不在一个网线端同时搭线到A、B通讯线上面？这样还不剩下一个接口？

其实细心的人已经发现，为啥不在一个短线端同时搭线到A、B通讯线上面，这样还不就一个接口？

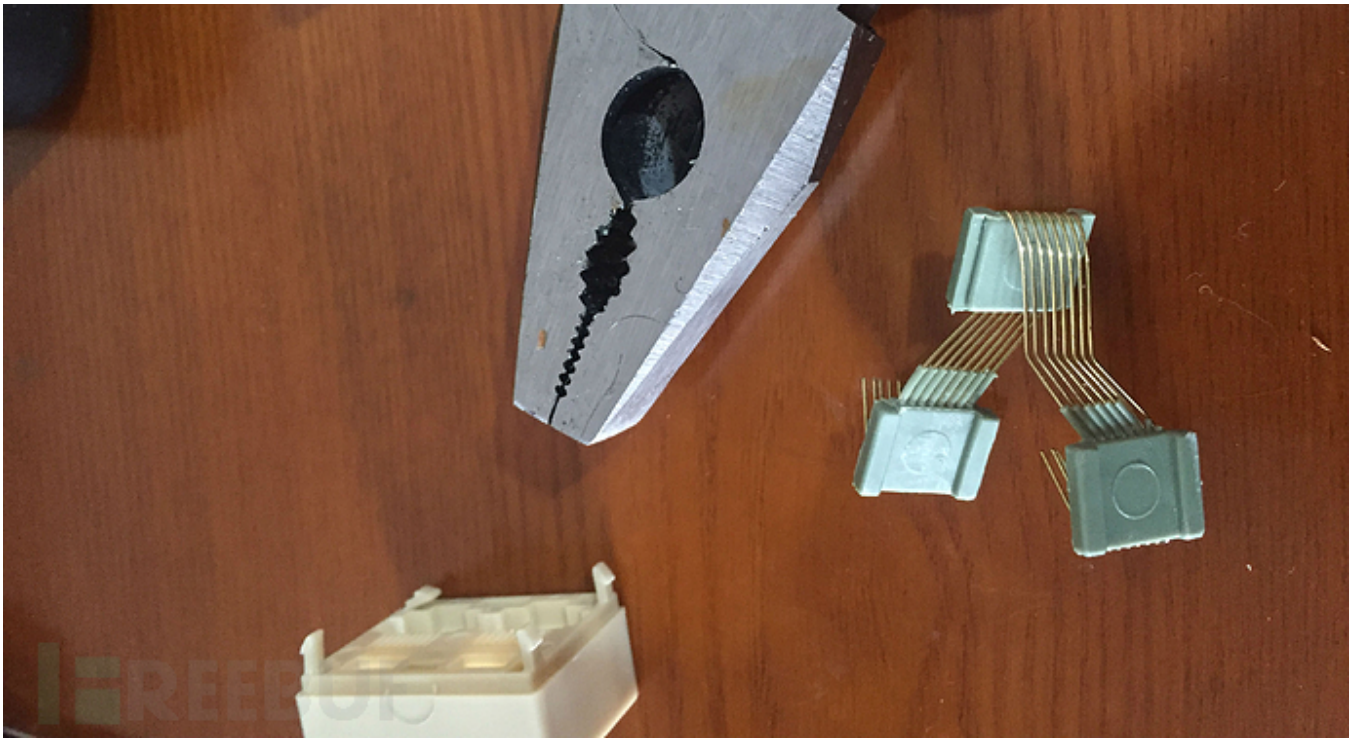
举个简单点比较容易理解的例子：

A同学和B同学隔着很远喊话，A问B 丫的你的密码多少？ B喊 123456 ，这时候你确实能够听到他的密码:123456也就是搭线了接收端能够听到，但如果B喊的同时你也对着A喊一句密码是：111111 ， 那么A这时候就听到两个人给出的答案，那么相信谁的？这就是通讯网络被搞混乱了。

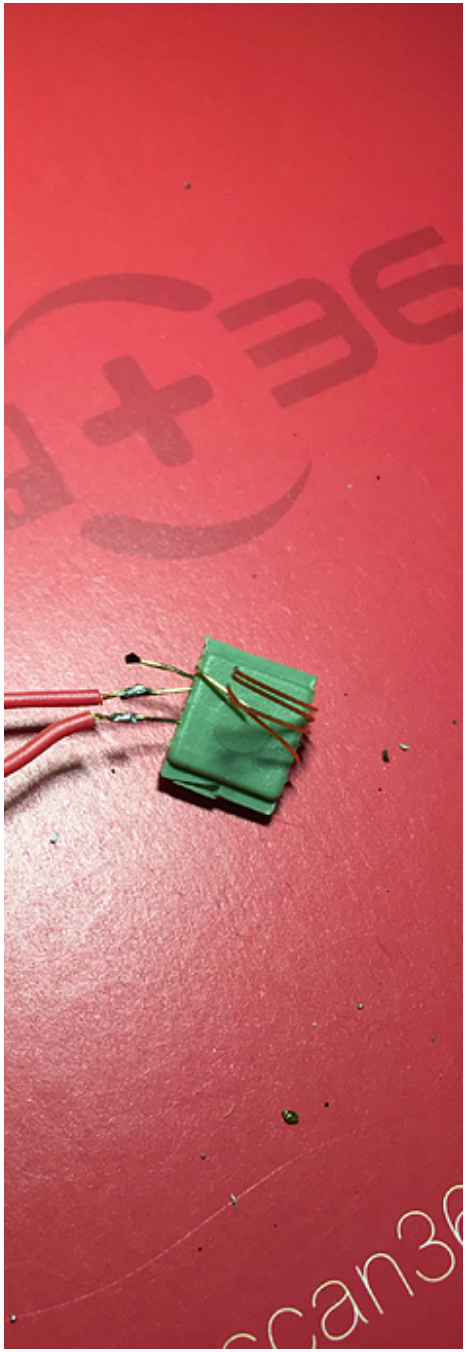
制作过程：

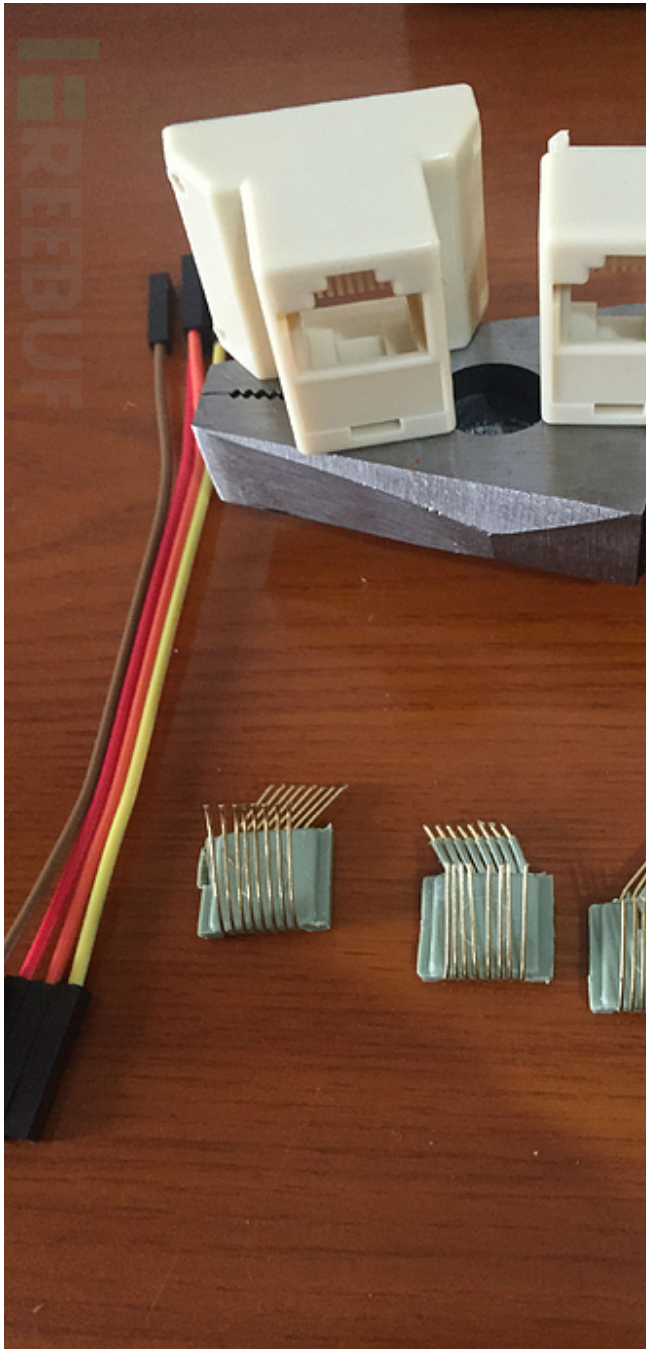
这里为了方便直接在五金部卖了一个一转二的接口，5毛钱。如图所示实物：

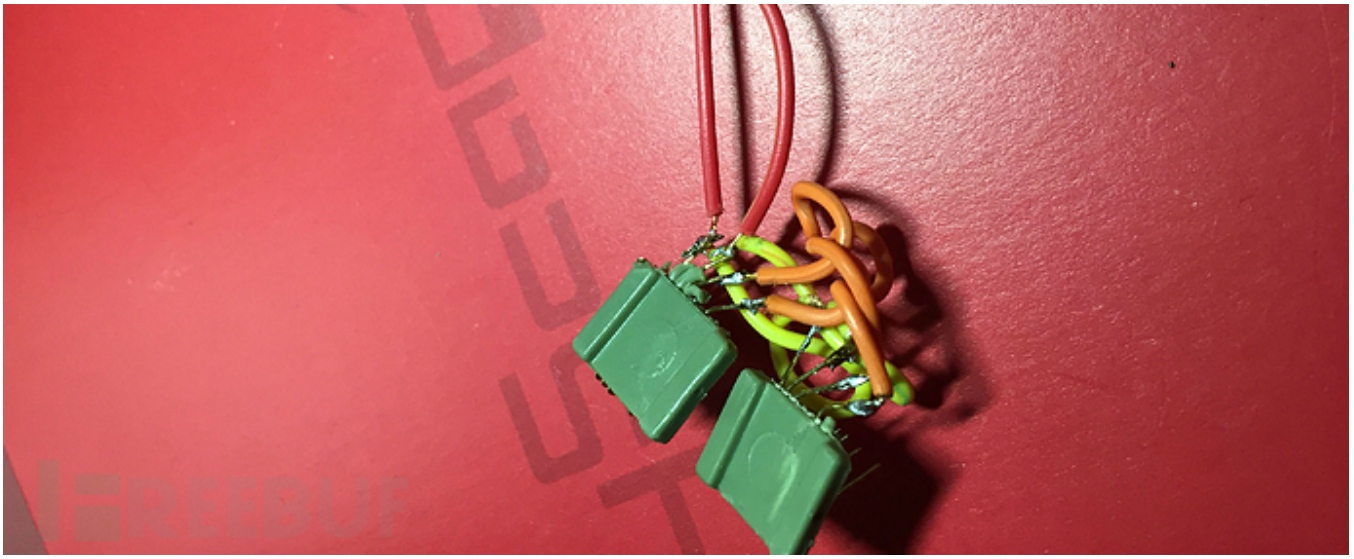
拆开后看下内部结构如下：



用老虎钳子分离后再用几根线 按照图上面的接线方式焊接起来如下两图：







OK 别问web “汪” 为啥有杜邦线，我不会告诉你上次写文章骗的金币换的~。~装好后接上线后在别的机器访问下qq.com 抓包瞅瞅，目测没有问题。

其实东西很简单，作为一个科普性的文章让大家可以花少量的钱就能玩点物理黑 ~。~

本文作者：creturn，转载请注明来自FreeBuf黑客与极客（FreeBuf.COM）