Apple portal弹窗报文

# 1. Portal弹窗是个啥？

简单的说就是当ios或是MacOS连接上需要认证的WiFi的时候系统会弹出一个窗口来进行wifi认证。

The Apple Captive Network Assistant (CNA) feature is an overlay that appears and prompts users automatically to login to the detected captive portal network without the need to explicitly open a web browser. This type of login is useful on mobile devices where many of the common applications are not browser-based and these applications would otherwise fail to connect without the successful browser-based authentication. Examples of these nonbrowser-based applications are email, social networking applications, corporate VPNs, and media streaming.

# 2. portal弹窗原理是啥？

The Apple operating systems detect the presence of a network that has captive portal enabled by attempting to request a web page from the Apple public website. This HTTP GET process retrieves a simple success.html file from the Apple web servers and the operating system uses the successful receipt of this file to assume that it is connected to an open network without the requirement for captive portal authentication.

If the success.html file is not received, the operating system conversely assumes that a captive portal is in place and presents the CNA automatically to prompt the user to perform a web authentication task. When the web authentication has completed successfully, the CNA window is closed automatically, which prevents the display of any subsequent welcome pages or redirecting of the user to their configured home page. If the user chooses to cancel the CNA, the Wi-Fi connection to the open network is dropped automatically, which prevents any further interaction via the full browser or other applications.

这里提到的web page就是http://captive.apple.com/hotspot-detect.html

当这个page返回success的时候就不会弹窗。

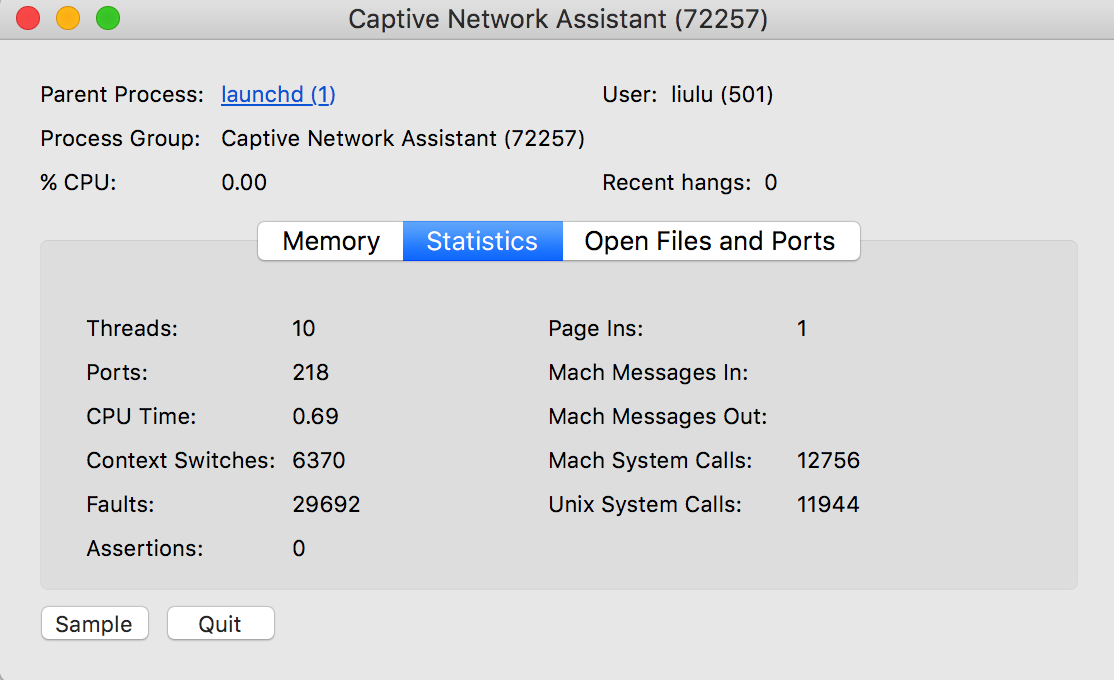
# 3. 抓包

抓包环境：MAC-PRO， wireshake，K2路由器

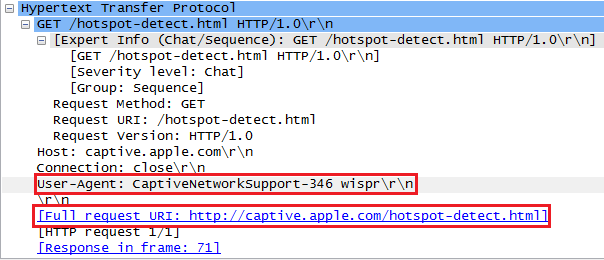
## 3.1 没有portal弹窗

配置K2为可以访问<http://captive.apple.com/hotspot-detect.html>

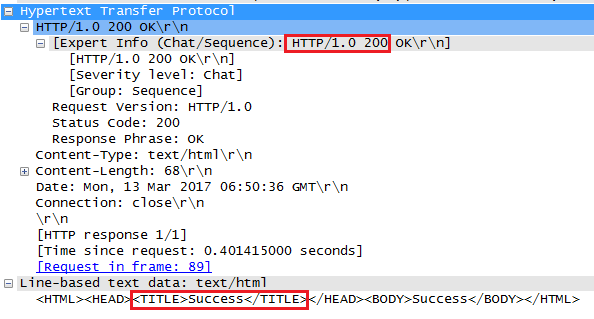
1. 连接上K2无线后系统会自动启动captive network assistant



2. captive network assistant会发出一个http请求，访问<http://captive.apple.com/hotspot-detect.html>



3. <http://captive.apple.com/hotspot-detect.html> 返回一个title为Success的网页。Ps，这里Success大小写敏感



当收到这个返回后，系统会认为不需要portal弹窗

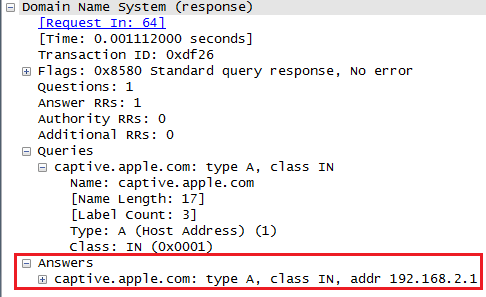
## 3.2 portal弹窗

将K2恢复出厂设置，然后连接K2 wifi

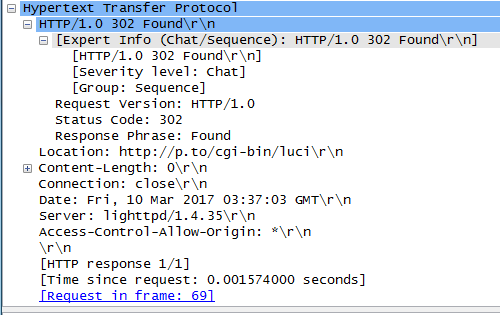
1. 连接上K2无线后系统会自动启动captive network assistant（同上）

2. captive network assistant会发出一个http请求，访问<http://captive.apple.com/hotspot-detect.html>（同上）

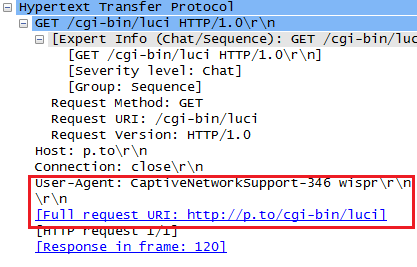
3. 路由器将DNS请求劫持到192.168.2.1上



4. 路由器的web服务器对http请求进行重定向



5. captive network assistant会显示重定向后p.to返回的信息



效果如下图：

