writeup wireshark

原创

PunkXiao 于 2018-04-17 20:24:06 发布 164 收藏
分类专栏： wireshark

本文链接：https://blog.csdn.net/qq_40273198/article/details/79980181


wireshark 专栏收录该内容
1 篇文章 0 订阅
订阅专栏

1.统计->对话 选择发包最多的会话作为过滤条件
2.发现bas64，iamge001.png

```
--B_3598538194_700708737
Content-type: image/png; name="image001.png";
 x-mac-creator="4F50494D";
 x-mac-type="504E4766"
Content-ID: <image001.png@01D38B05.8079CE40>
Content-disposition: inline;
          filename="image001.png"
Content-transfer-encoding: base64

iVBORw0KGgoAAAANSUhEUgAABIwAAAISCAYAAACu6lSmAAAMKGlDQ1BJQ0MgUHJvZmlsZQAA
SImVVwdYU8kWnluSkJDQAhGQEnoTpVepoUUQkCrYCEkgocSYEETsyKKCa0HFghVZFVFwLYAs
NixYWBTs9WFBRVkXCzZU3iQBdPV7733vfN+5979nzpz5z7kz880AoB7NEYuzUA0AskU5kpjQ
QObEpGQm6SFAAArIwBM4crhScUB0dASAMvT+p7y7Dr2hXLGXx/q5/b+KJo8v5QKAREOcypNy
syE+BADuxhVLcgAg9EC72cwcMcREyBJoSyBBiM31OF2JPeQ4VYkjFD5xMSyIUwBQoXI4knQA
1OS8mLncdBhHbRnEDiKeUARxE8S+XAGHB/FniEd1Z0+HWN0aYuvU7+Kk/yNm6nBMDid9GCtz
UYhKkFAqzuLM+j/L8b8lO0s2NIYZVKpAEhYjz11et8zp4XJMhficKDUyCmItiK8KeQp/OX4i
kIXFD/p/4EpZsGaAAQBK5XGCwiE2gNhUlBUZMWj3TROGsCGGtUfjhDnsOGVflCeZHjMYH83j
S4NjhzBHohhLZlMsv4wPGIv5RcBnD8VszBfEJSn5onqzbQmREKtBfEeaGRs+6PM8X8CKHPKR
```


将base64文件解码为图片
base64解码地址：https://www.base64decode.org/

```
MIICXAIBAAKBgQDCm6vZmclJrVH1AAyGuCuSSZ8O+mIQiOUQCvN0HYbj8153JfSQ
LsJIhbRYS7+zZ1oXvPemWQDv/u/tzegt58q4ciNmcVnq1uKiygc6QOtvT7oiSTyO
vMX/q5iE2iClYUIHZEKX3BjjNDxrYvLQzPyGD1EY2DZIO6T45FNKYC2VDwIDAQAB
AoGAbtWUKUkx37lLfRq7B5sqjZVKdpBZe4tL0jg6cX5Djd3Uhk1inR9UXVNw4/y4
QGfzYqOn8+Cq7QSoBysHOeXSiPztW2cL09ktPgSlfTQyN6ELNGuiUOYnaTWYZpp/
QbRcZ/eHBulVQLlk5M6RVs9BLI9X08RAl7EcwumiRfWas6kCQQDvqC0dxl2wIjwN
czILcoWLig2c2u71Nev9DrWjWHU8eHDuzCJWvOUAHIrkexddWEK2VHd+F13GBCOQ
ZCM4prBjAkEAz+ENahsEjBE4+7H1HdIaw0+goe/45d6A2ewO/lYH6dDZTAzTW9z9
kzV8uz+Mmo5163/JtvwYQcKF39DJGGtqZQJBAKa18XR16fQ9TFL64EQwTQ+tYBzN
+04eTWQCmH3haeQ/0Cd9XyHBUveJ42Be8/jeDcIx7dGLxZKajHbEAfBFnAsCQGq1
AnbJ4Z6opJCGu+UP2c8SC8m0bhZJDelPRC8IKE28eB6SotgP61ZqaVmQ+HLJ1/wH
/5pfc3AmEyRdfyx6zwUCQCAH4SLJv/kprRz1a1gx8FR5tj4NeHEFFNEgq1gmiwmH
2STT5qZWzQFz8NRe+/otNOHBR2Xk4e8IS+ehIJ3TvyE=
```


提取图片中文字得到RSA密钥，根据提示补齐格式

```
-----BEGIN RSA PRIVATE KEY-----
XXXXXXX
-----END RSA PRIVATE KEY-----
```


3.将密钥导入wireshark
编辑->首选项->protocols->ssl->

IP address	Port	Protocol	Key File	Password
	443	http	C:/Users/Administrator/Desktop/rsa_key.txt	

4.过滤出流量包中ssl对话
追踪ssl流，得到flag