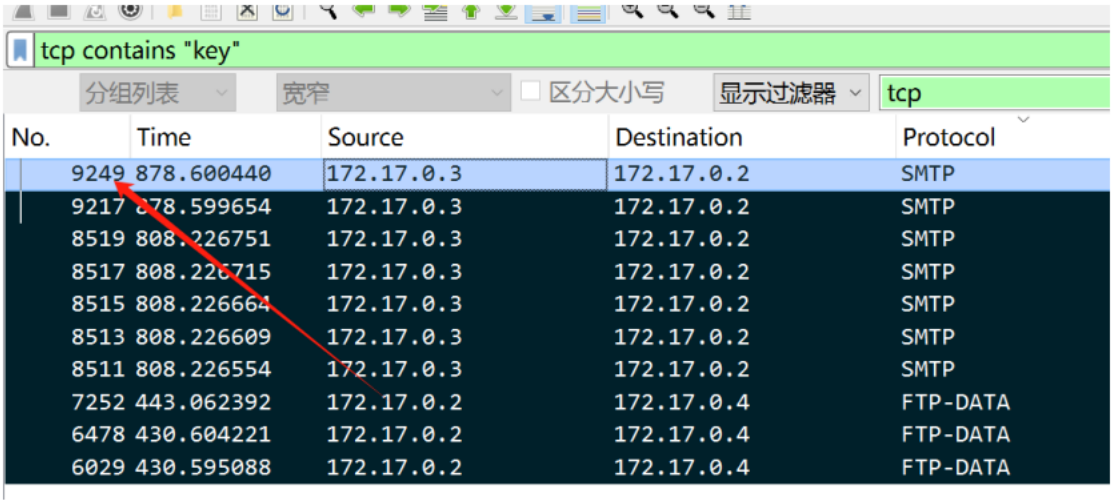
流量分析七

http://www.ctf8.com/index/containers/ContainerOtherCtfDetail/52
根据提示去找 key，
在 tcp 流量中过滤 key：tcp contains "key"
追踪几条 发现：

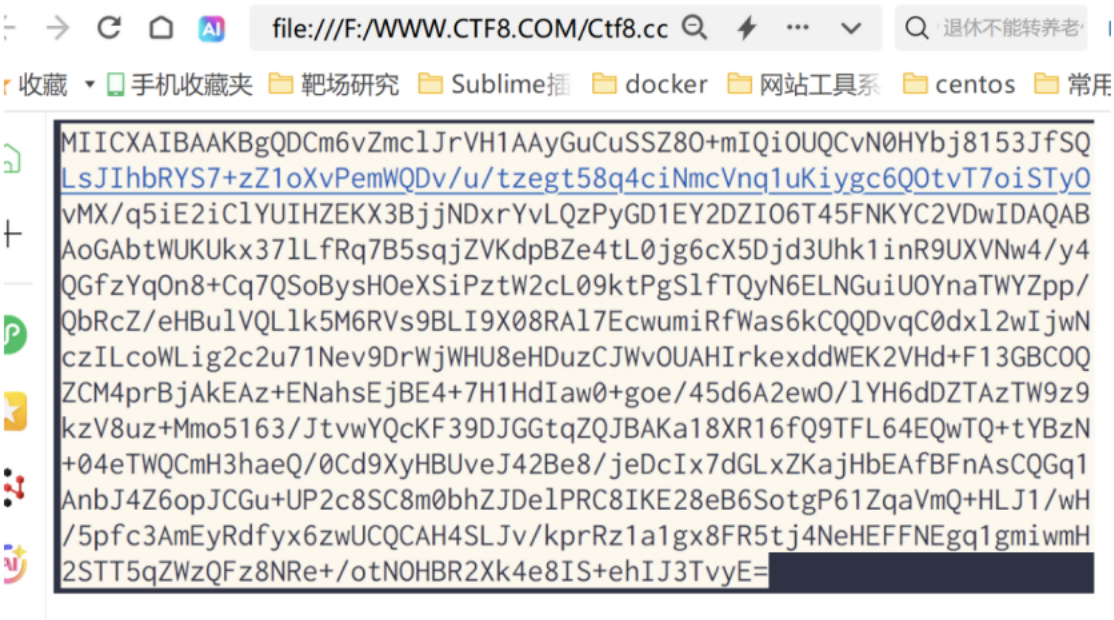



```
--B_3598538194_2172270964--


--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

iVBORw0KGgoAAAANSUhEUgAABIwAAAISCAYAAACu61SmAAAMKGlDQ1BJQ0MgUHJvZmlsZQAA
SImVVwdYU8kWnluSkJDQAhGQEnoTpVepoUUQkCrYCEkgocSYEETsyKKCa0HFghVZFVFwLYAs
NixYWBTs9WFBRVkXCzZU3iQBdPV7733vfN+5979nzpz5z7kz880AoB7NEYuzUA0AskU5kpjQ
QObEpGQm6SFAAArIwBM4crhScUB0dASAMvT+p7y7Dr2hXLGXx/q5/b+KJo8v5QKAREOcypNy
syE+BADuxhVLcgAg9EC72cwcMcREyBJoSyBBiM3lOF2JPeQ4VYkjFD5xMSyIUwBQoXI4knQA
1OS8mLncdBhHbRnEDiKeUARxE8S+XAGHB/FniEd1Z0+HWN0aYuvU7+Kk/yNm6nBMDid9GCtz
UYhKkFAqzuLM+j/L8b8lO0s2NIYZVKpAEhYjz11et8zp4XJMhficKDUyCmItiK8KeQp/OX4i
kIXFD/p/4EpZsGaAAQBK5XGCwiE2gNhUlBUZMWj3TROGsCGGtUfjhDnsOGVflCeZHjMYH83j
S4NjhzBHohhL7lMsy4wPGIy5RcBnD8VszBfEJSp5opdzhQmREKtBfFeaGRs+6PM8X8CKHPKR
yGLknOE/x0CaJCRG6YOZZ0uH8sK8BEJ25CCOyBHEhSn7Yl05HAU3XYgz+NKJEUM8efygYGVe
WAFfFD/IHysV5wTGDPpXirOiB/2xJn5WqNxuCnGbNDd2qG9vDpxsynxxIM6Jj1Nyw7UzOOOi
lRxwWxABWCAIMIEMaiqYDjKAsK2nvgd+KVtCAAdIQDrgA/tBy1CPREWLCD5jQT74CyI+kA73
C1S08kEutH8Ztiqf9iBN0Zqr6JEJnkCcDcJBFvyWKXqJhkdLAI+hRfjT6FzINQuqvO0nG1N9
yEYMJgYRw4ghRBtcH/fFvfEI+PSH6oR74J5DvL75E54Q2gkPCdcInYRb04QFkh+YM8F40Ak5
hgxml/p9drgljOqKB+I+MD6MjTNwfWCPu8CRAnA/OLYrtH7PVTac8bdaDsYiO5BR8giyP9n6
RwZqtmquw1Hklfq+FkpeqcPVYg23/JgH67v68eA7/EdPbAl2EGvBTmLnsSasHjCx41gD1ood
lePhufFYMTeGRotR8MmEcYQ/jccZHFNeNalDtUO3w+fBNpDDz8uRLxbWdPEsiTBdkMMMgLs1
n8kWcUePYjo5OMJdVL73K7eWNwzFno4wLnyzFewAwMd3YGCg6ZstvAuAg70AUO59s1nDdajW
AcC5NVyZJFdpw+UPAqAAdbhS9IAR3LusYUZOwA14A38QDMaBKBAHksBUWGcBnKcSMBPMAQtB
```

补头：之后 base64 转图片
简历 HTML 文件，如下图

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title></title>
</head>
<body>
<img src="
SImVVwdYU8kWnluSkJDQAhGQEnoTpVepoUUQkCrYCEkgocSYEETsyKKCa0HFghVZFVFwLYAs
NixYWBTs9WFBRVkXCzZU3iQBdPV7733vfN+5979nzpz5z7kz880AoB7NEYuzUA0AskU5kpjQ
QObEpGQm6SFAAArIwBM4crhScUB0dASAMvT+p7y7Dr2hXLGXx/q5/b+KJo8v5QKAREOcypNy
syE+BADuxhVLcgAg9EC72cwcMcREyBJoSyBBiM3lOF2JPeQ4VYkjFD5xMSyIUwBQoXI4knQA
1OS8mLncdBhHbRnEDiKeUARxE8S+XAGHB/FniEdlZO+HWN0aYuvU7+Kk/yNm6nBMDid9GCtz
UYhKkFAqzuLM+j/L8b8lOOs2NIYZVKpAEhYjz1let8zp4XJMhficKDUyCmItiK8KeQp/OX4i
kIXFD/p/4EpZsGaAAQBK5XGCwiE2gNhUlBUZMWj3TROGsCGGtUfjhDnsOGVflCeZHjMYH83j
S4NjhzBHohhL7lMsy4wPGIy5RcBnD8VszBfEJSp5opdzhQmREKtBfFeaGRs+6PM8X8CKHPKR
```

运行如图：



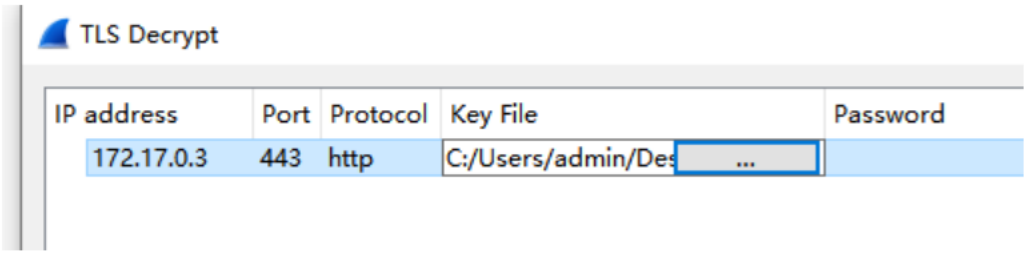
识别图片内容，补齐私钥：

-----BEGIN RSA PRIVATE KEY-----

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=
-----END RSA PRIVATE KEY-----
保存成 txt 文件

回到流量分析图中，随便选中 tlsv1.2 协议流量，右键，选择“协议首选项”中“Transport Layer Security”中
“RSA keys list”



加载后 追踪 http 流量，得 flag
DDCTF{0ca2d8642f90e10efd9092cd6a2831c0}