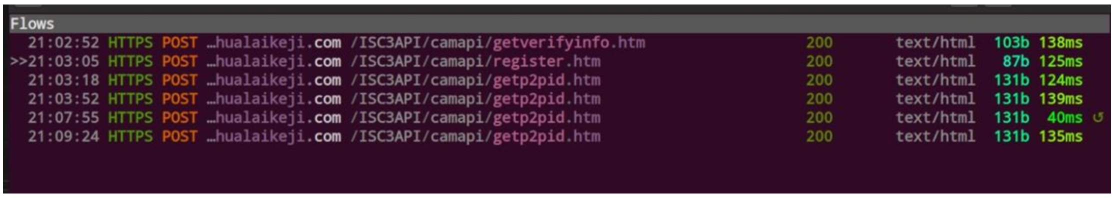
Hualai Xiaofang camera

Model: iSC5

Firmware: 3.2.2_112

The application does not call any certificate verification APIs to verify the server certificate and make the application vulnerable to Man-in-the-middle attack. The following figure shows we can decrypt the traffic with Man-in-the-middle attack.



```
Flows
  21:02:52 HTTPS POST …hualaikeji.com /ISC3API/camapi/getverifyinfo.htm        200       text/html  103b 138ms
>>21:03:05 HTTPS POST …hualaikeji.com /ISC3API/camapi/register.htm             200       text/html   87b 125ms
  21:03:18 HTTPS POST …hualaikeji.com /ISC3API/camapi/getp2pid.htm             200       text/html  131b 124ms
  21:03:52 HTTPS POST …hualaikeji.com /ISC3API/camapi/getp2pid.htm             200       text/html  131b 139ms
  21:07:55 HTTPS POST …hualaikeji.com /ISC3API/camapi/getp2pid.htm             200       text/html  131b  40ms ↺
  21:09:24 HTTPS POST …hualaikeji.com /ISC3API/camapi/getp2pid.htm             200       text/html  131b 135ms
```

Our manual analysis shows that this vulnerability affects the device login process of the camera. When connecting to the Internet, the device tries to login to the cloud server, so that its user could control the camera through the cloud. In the login request, we observe a key named “camenr” which has 16 characters. The key is used to represent the identity of the device and has been registered to the cloud previously during the device binding. With this key, the cloud could recognize the owner of a connected device. By manipulating the “camenr” key, we successfully conduct a denialof-login attack for a victim camera through a MITM proxy. In this attack, we hijack the SSL/TLS connection for the login request and modify the original “camenr” field to a wrong value. Then, though the device has been connected to the Internet, its user cannot find the device through the cloud and cannot use it properly.