Sniffing the plain-text traffic in Xiongmai Camera

@ladinas, @chandlerchen

Affected versions:

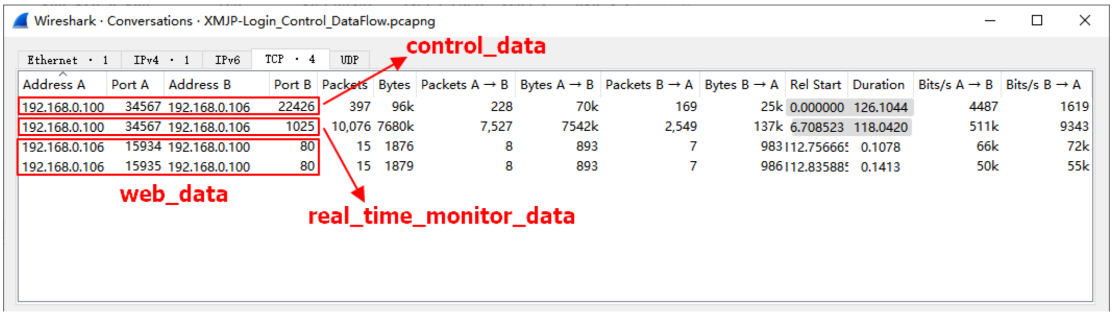
Version ≤ V4.02.R12.A6420987.10002.147502.00000

Proof of Concept:

1, open the wireshark, monitor the same network which the camera locates.

2, browse the web app of the camera, log in the account with the username/password you set before.

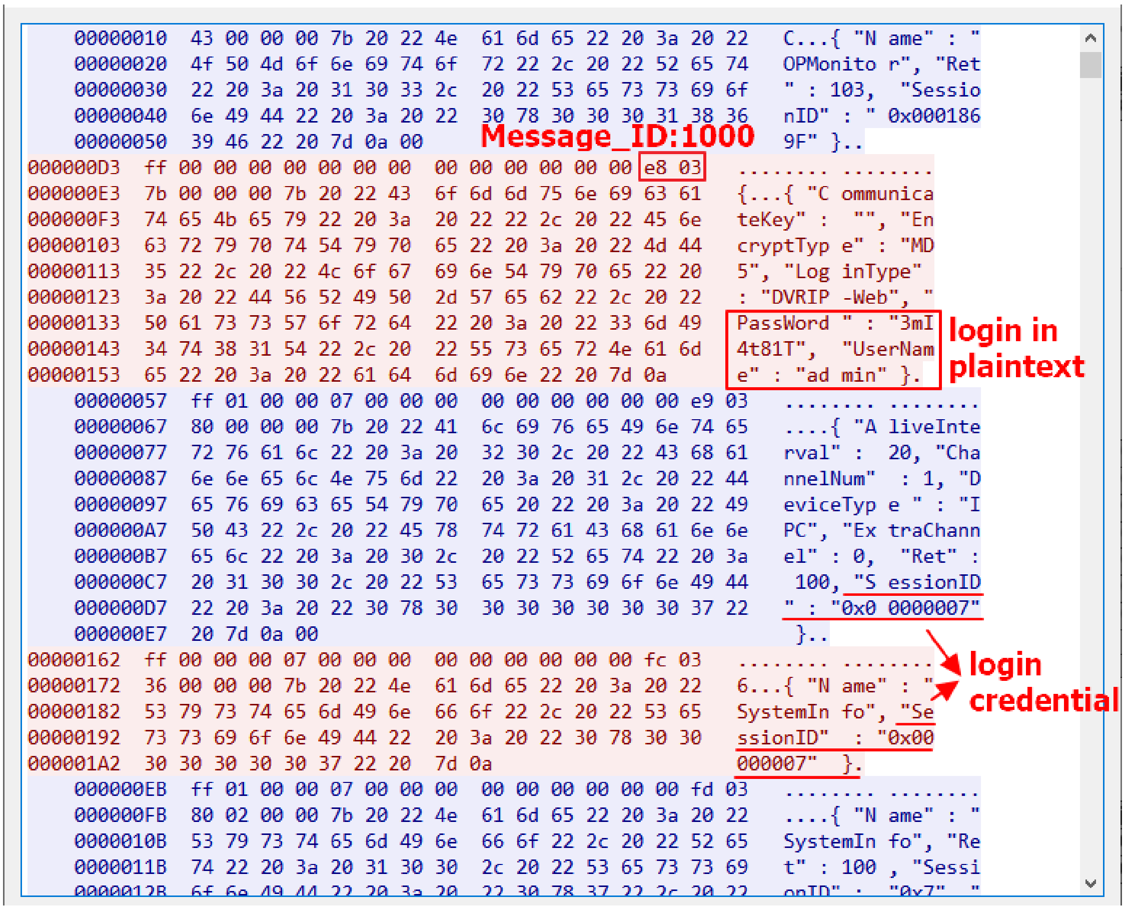
3, you could find control data, web data and real-time monitoring data together.



Wireshark · Conversations · XMJP-Login_Control_DataFlow.pcapng

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.0.100	34567	192.168.0.106	22426	397	96k	228	70k	169	25k	0.000000	126.1044	4487	1619
192.168.0.100	34567	192.168.0.106	1025	10,076	7680k	7,527	7542k	2,549	137k	6.708523	118.0420	511k	9343
192.168.0.106	15934	192.168.0.100	80	15	1876	8	893	7	983	112.75666!	0.1078	66k	72k
192.168.0.106	15935	192.168.0.100	80	15	1879	8	893	7	986	112.83588!	0.1413	50k	55k

4. try to analyze the control data. All the contents are in plain text, which can be easily sniffed.



```
    00000010  43 00 00 00 7b 20 22 4e  61 6d 65 22 20 3a 20 22   C...{ "N ame" : "
    00000020  4f 50 4d 6f 6e 69 74 6f  72 22 2c 20 22 52 65 74   OPMonito r", "Ret
    00000030  22 20 3a 20 31 30 33 2c  20 22 53 65 73 73 69 6f   " : 103,  "Sessio
    00000040  6e 49 44 22 20 3a 20 22  30 78 30 30 30 31 38 36   nID" : " 0x000186
    00000050  39 46 22 20 7d 0a 00                               9F" }..
000000D3  ff 00 00 00 00 00 00 00  00 00 00 00 00 00 e8 03   ........ ........
000000E3  7b 00 00 00 7b 20 22 43  6f 6d 6d 75 6e 69 63 61   {...{ "C ommunica
000000F3  74 65 4b 65 79 22 20 3a  20 22 22 2c 20 22 45 6e   teKey" :  "", "En
00000103  63 72 79 70 74 54 79 70  65 22 20 3a 20 22 4d 44   cryptTyp e" : "MD
00000113  35 22 2c 20 22 4c 6f 67  69 6e 54 79 70 65 22 20   5", "Log inType"
00000123  3a 20 22 44 56 52 49 50  2d 57 65 62 22 2c 20 22   : "DVRIP -Web", "
00000133  50 61 73 73 57 6f 72 64  22 20 3a 20 22 33 6d 49   PassWord " : "3mI
00000143  34 74 38 31 54 22 2c 20  22 55 73 65 72 4e 61 6d   4t81T",  "UserNam
00000153  65 22 20 3a 20 22 61 64  6d 69 6e 22 20 7d 0a      e" : "ad min" }.
    00000057  ff 01 00 00 07 00 00 00  00 00 00 00 00 00 e9 03   ........ ........
    00000067  80 00 00 00 7b 20 22 41  6c 69 76 65 49 6e 74 65   ....{ "A liveInte
    00000077  72 76 61 6c 22 20 3a 20  32 30 2c 20 22 43 68 61   rval" :  20, "Cha
    00000087  6e 6e 65 6c 4e 75 6d 22  20 3a 20 31 2c 20 22 44   nnelNum"  : 1, "D
    00000097  65 76 69 63 65 54 79 70  65 20 22 20 3a 20 22 49   eviceTyp e " : "I
    000000A7  50 43 22 2c 20 22 45 78  74 72 61 43 68 61 6e 6e   PC", "Ex traChann
    000000B7  65 6c 22 20 3a 20 30 2c  20 22 52 65 74 22 20 3a   el" : 0,  "Ret" :
    000000C7  20 31 30 30 2c 20 22 53  65 73 73 69 6f 6e 49 44    100, "S essionID
    000000D7  22 20 3a 20 22 30 78 30  30 30 30 30 30 30 37 22   " : "0x0 0000007"
    000000E7  20 7d 0a 00                                         }..
00000162  ff 00 00 00 07 00 00 00  00 00 00 00 00 00 fc 03   ........ ........
00000172  36 00 00 00 7b 20 22 4e  61 6d 65 22 20 3a 20 22   6...{ "N ame" : "
00000182  53 79 73 74 65 6d 49 6e  66 6f 22 2c 20 22 53 65   SystemIn fo", "Se
00000192  73 73 69 6f 6e 49 44 22  20 3a 20 22 30 78 30 30   ssionID"  : "0x00
000001A2  30 30 30 30 30 37 22 20  7d 0a                     000007"  }.
    000000EB  ff 01 00 00 07 00 00 00  00 00 00 00 00 00 fd 03   ........ ........
    000000FB  80 02 00 00 7b 20 22 4e  61 6d 65 22 20 3a 20 22   ....{ "N ame" : "
    0000010B  53 79 73 74 65 6d 49 6e  66 6f 22 2c 20 22 52 65   SystemIn fo", "Re
    0000011B  74 22 20 3a 20 31 30 30  2c 20 22 53 65 73 73 69   t" : 100 , "Sessi
    0000012B  6f 6e 49 44 22 20 3a 20  22 30 78 37 22 2c 20 22   onID" :  "0x7", "
```

5. Just as showed above, the plain password is “3mI4t81T”, while we set the default password “1qazxsw2”. The encoded one could acquire through Dahua camera encoding toolset (https://github.com/haicenhacks/DahuaHashCreator), which means hacker can sniff the authentication process and monitor all the actions online.