

Hacking your printer
for free and...

wtflolq?!

by Fist0urs <eddy.maaalou@gmail.com>





ip.addr==192.168.

Expression... +

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------|-------------|----------|--------|--|
| 13 | 14.349693 | 192.168. | 192.168. | BJNP | 58 | Scanner Command: Discover |
| 16 | 14.354409 | 192.168. | 192.168. | BJNP | 74 | Scanner Response: Discover |
| 17 | 14.356112 | 192.168. | 192.168. | BJNP | 158 | Scanner Command: Scan Job Details |
| 18 | 14.357994 | 192.168. | 192.168. | BJNP | 110 | Scanner Response: Scan Job Details |
| 19 | 14.358998 | 192.168. | 192.168. | BJNP | 158 | Scanner Command: Scan Job Details |
| 20 | 14.361926 | 192.168. | 192.168. | BJNP | 110 | Scanner Response: Scan Job Details |
| 21 | 14.362944 | 192.168. | 192.168. | BJNP | 174 | Scanner Command: Scan Job Details |
| 22 | 14.364786 | 192.168. | 192.168. | BJNP | 110 | Scanner Response: Scan Job Details |
| 56 | 18.368240 | 192.168. | 192.168. | BJNP | 174 | Scanner Command: Scan Job Details |
| 57 | 18.370137 | 192.168. | 192.168. | BJNP | 110 | Scanner Response: Scan Job Details |
| 60 | 22.371346 | 192.168. | 192.168. | BJNP | 174 | Scanner Command: Scan Job Details |
| 61 | 22.373222 | 192.168. | 192.168. | BJNP | 110 | Scanner Response: Scan Job Details |
| 62 | 26.375299 | 192.168. | 192.168. | BJNP | 174 | Scanner Command: Scan Job Details |
| 63 | 26.378592 | 192.168. | 192.168. | BJNP | 110 | Scanner Response: Scan Job Details |
| 64 | 28.631201 | 192.168. | 192.168. | BJNP | 58 | Printer Command: Discover |
| 65 | 28.641555 | 192.168. | 192.168. | BJNP | 74 | Printer Response: Discover |
| 66 | 28.659208 | 192.168. | 192.168. | BJNP | 62 | Printer Command: Get Printer Identity |
| 67 | 28.675346 | 192.168. | 192.168. | BJNP | 254 | Printer Response: Get Printer Identity |
| 68 | 28.682259 | 192.168. | 192.168. | BJNP | 450 | Printer Command: Print Job Details |
| 69 | 28.714012 | 192.168. | 192.168. | BJNP | 62 | Printer Response: Print Job Details |
| 70 | 28.714856 | 192.168. | 192.168. | TCP | 66 | 4738 → 8611 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 71 | 28.720750 | 192.168. | 192.168. | BJNP | 62 | Printer Command: Get Printer Identity |
| 72 | 28.727485 | 192.168. | 192.168. | TCP | 60 | 8611 → 4738 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 |
| 73 | 28.727642 | 192.168. | 192.168. | BJNP | 254 | Printer Response: Get Printer Identity |
| 74 | 28.727655 | 192.168. | 192.168. | TCP | 54 | 4738 → 8611 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 75 | 28.733622 | 192.168. | 192.168. | TCP | 78 | 4738 → 8611 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=24 |
| 76 | 28.736584 | 192.168. | 192.168. | TCP | 60 | 8611 → 4738 [ACK] Seq=1 Ack=25 Win=65511 Len=0 |
| 77 | 28.763730 | 192.168. | 192.168. | TCP | 60 | 58565 → 5357 [SYN] Seq=0 Win=11520 Len=0 MSS=1460 |

▶ Frame 66: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0

▶ Ethernet II, Src: Giga-Byt_ (), Dst: _e6:78:3e ()

▶ Destination: _e6:78:3e ()

▶ Source: Giga-Byt_ ()

Type: IPv4 (0x0800)

▶ Internet Protocol Version 4, Src: 192.168. Dst: 192.168.

▶ User Datagram Protocol, Src Port: 65285 (65285), Dst Port: 8611 (8611)

▶ Canon BJNP, Printer Command: Get Printer Identity

Id: BJNP

Type: Printer Command (1)

Code: Get Printer Identity (48)

Sequence Number: 1

Session Id: 0

Payload Length: 4

```

0000 88 87 17 e6 78 3e 94 de 80 6b 02 e3 08 00 45 00  ....x>.. .k...E.
0010 00 30 38 a5 00 00 80 11 00 00 c0 a8 2a 0d c0 a8  .08.....*...
0020 2a 31 ff 05 21 a3 00 1c d5 bc 42 4a 4e 50 01 30  *1.!... .BJNP.0
0030 00 00 00 01 00 00 00 00 00 04 80 00 00 00 00  .....

```

```
C.JG.....GjA.j.QE'.K....
.Q@.f....8.....9....H[.4.)h>.u.K.....t...;Q:...w.GZ;Q@.w.E....4.....J:u..4{.3E---E&iA=.1G.x.x...z3....
(.....&h...h.)sF(.P.=(.....a.....):PzP.I.K.(.....~4v...
...F(...&(.~4.R..."t....h$.zw..Rg..(<..ZCE=1@..QF)q..%.....#...I..P...4..
..QE..3KE.;i23k@.....4..E.)?(...(..zP@.I.-.....N.g..1@.z?
^..h....Gnh.....P.c.Q.....#.....z.....)GJZ>...f..s..Q@..4QK.j...g....
(.4....C@..Gnh.FiO.....qH(...i9...Q...Fh.@.....(i;.....(4.R.b...qK.P.I.)h.9...J.L{.....3KE...4c.
(..M.....~4}h.....?Z);...b...b..P...-RP...9...QH)h.w.E~.;FE.f...g...(...=h...Nh...-E&)
{P.R...N...~...z;.h...P:....v...(>..
..h..P..3.'.Gj.\I.(.....H. 9.....ZO...ZNS....g.....~U.y.t....
-7.<S.QE.....?Z):.R.....w...@'=)qI@.E.s@..4.Q...R...3A...Rf..t.....g.)?
.Z;u.<P:P..u..%/4.q.....
1H84...}i.;KG~(...(>.....G9..@.4v..J(.QGj.J(.G.{.KIG4.....P(@..&A&....
-.9.G.E...?Z\E...=h..4f.....P...t..4.df..u4P1K.....g.S...?.9...u....)...4R...;Rf.%-'z...P.E.w...4QFy.4.
;...;.....j.Z.M....?.(...c.....h...sFx..I..3.>.....(.)y..J..b...s384.....i{.....&1....x...
4.....s.2q@...&
.....:R
1...u.J.4.....rh.Gz.;h.M/C.....z.....!Jh=(.c.....zPzP@.h.(.....b.....J:R...ZO.Gz;..h.K.;!..qA.H....4PqG...
....g.;Q.....^..b.t.....^.....t.....w.Q.h.9.G=/.....'...=iz.h8...!..Q.(.4...F)h.E.....SFFr8.....4.sGjA...P.
4...g....;K..f....K...w..J.....o.....\..~....K.
mF@.x...Vp...^...'7.+.....4.Q.#.>.8.EN9\TK.....@.1H.P.^).....3GQH.g.J...J(.W.....~...OnigZA....
4..SG...~c.N....!..A.....@..i3.....!....PzP{R...J.R~ZB2(9...@..4.....q@..R.R...[.J...(.7...$-...O.R)..N...B.j....3L
.Iu,!!}.u5..Kr.}p*P.i9--
.x.)A.G.P...sGS.Z.9.....I..pB.@...}{.L.....i;b...y..R.....
1.....x.B.;.HH...#.ai6..m.'.....Z.ZSM'..._...
zsA.E.....F=.)...@.....v...R~4g.@
(.@sK.@...E.....!i..M.4..=-.4...aA...G..=(...>..(.....v..x...J=.4..(.@..@<..=.4.P84...@
.....J.N.b.@.z...PG..PzRR...o.....(....
(...ix.g.(.....;J3..w.@.....B>...=3Gj^h.Rv./j.'n.v.K....Z^.:Q...h...z..h..w..m...N....s..9.@.CGz;...
....q.@...
...v.@..}GJJ1.;Q.R.....Q.....Q@...;...i){.A...w...1G.Q.(....QE....(.('z.8..{.
1;..Q...i8....f...F}..h.4bBJNP...>.....>.....BJNP...>.....0.....Q.9...;Q.
...qE.....`...@.9.QE.&9..Gz..BJNP.!...>.....>.....BJNP.!...>.....>.....BJNP...>.....BJNP.
.....>.....>.....BJNP.!...>.....>.....BJNP.!...>.....>.....BJNP...>.....BJNP.
.....>.....>.....BJNP.!...>.....>.....BJNP.!...>.....>.....BJNP...>.....BJNP.
.....>.....>.....BJNP.!...>.....>.....BJNP.!...>.....>.....BJNP...>.....BJNP.
.....>.....>.....BJNP.!...>.....>.....BJNP.!...>.....>.....BJNP...>.....BJNP.
.....>.....>.....BJNP.!...>.....>.....BJNP.!...>.....>.....BJNP...>.....BJNP.
.....>.....>.....BJNP.!...>.....>.....BJNP.!...>.....>.....BJNP...>.....BJNP.
.....>.....>.....BJNP.!...>.....>.....BJNP.!...>.....>.....BJNP...>.....BJNP.
.....>.....>.....@...A..b..bs.....Rs.u.....O.....c4.%...u..q@./z(.u.4w.P.h.^...w.RP.E.@.....
B.8...v..QGj?
..J.....w.....)h.;...J^..w.....(..H.8...f.M.....j^i;Q./4s.h.h.%-.....QA.@...I.-%.
SM...@.I.)h.@..v...
1@<Q.P.GJ?
9.@.JL{.....qI.ZJ.f.....Q.i.{.1M.Q@..J(@..)...SN9.....G8...R.&..KE&
..-.....-.....!.....h}.G4w...:P.IG.P.`.KA..:P.R.s..3G'.ZN.w...:0.3.....
...ZO..4P...Q.....Gn.b...c..{..G4Q..C.....3.....bR.Gz.Q..1@...O.P.R.b....E.P!(-.
<P@..Gz.=KF.....!K...LR...Z1.JJ(.QE.....ZNh.t...\. (....;P.'=(.....sI..P..G.....v..
(.=iy..@..Q@..g.;P..h..J;....@..w.A.B.)i)h.R.c&..Nwg./j)M.....
```

1 273 client pkt(s), 2 508 server pkt(s), 2545 tours.

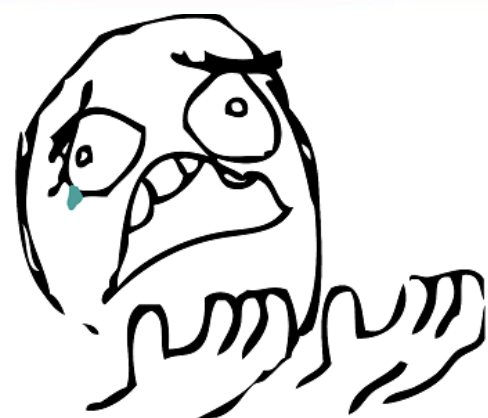
Entire conversation (2086 kB) Afficher les données comme ASCII Flux 12

Trouver: Trouver Suivant

Cacher ce flux Imprimer Save as... Close Help

```
BJNP.....BJNP.....BJNP.....BJNP.....SRC80;100;.....BJNP.....BJNP.....S
RC80;100;...u...<adminid>ADMIN</adminid><pswdon>1</pswdon><pswd><![CDATA[6978627a335133364b5578743251594b59386573 ]]></pswd><firmver>1.050</
firmver><firmUSBupdate>0</firmUSBupdate><firmLANupdate>0</firmLANupdate><extmode>00</extmode><maxNUM>0</maxNUM><macfilteron>0</macfilteron><macfilter></
macfilter><ipfilteron>0</ipfilteron><ipfilter></ipfilter><WSDon>1</WSDon><enableLAN>1</enableLAN><param_set><ID><![CDATA[wireless0]]></ID><friendlyname></
friendlyname><ifenable>1</ifenable><linkactive>1</linkactive><802.11><IFtype>n</IFtype><wlmode>infra</wlmode><ssid><
ssid><bssid>FFFFFFFF</bssid><ch>6</ch><wepon>0</wepon><weplength>64</weplength><wepformat>STRING</wepformat><auth>AUTO</auth><wepid>1</wepid><wep1></
wep1><wep2></wep2><wep3></wep3><wep4></wep4><pwrnmng>0</pwrnmng><wpaon>0</wpaon><wpamode>EAP/PSK</wpamode><wpa_encrypt>CCMP</wpa_encrypt><wpa2on>1</
wpa2on><wpa2_encrypt>CCMP</wpa2_encrypt><wpa_psk>757e602f782b32625278412b4a7a6131217a3d56</wpa_psk><setbssidenable>1</
setbssidenable><searchparamenable>1</searchparamenable></802.11><IP><ipmode>MANUAL</ipmode><ipaddress>192.168.
ipaddress><hwaddress>
</hwaddress><submask>255.255.255.0</submask><gateway>192.168.
:/gateway><ipv6on>0</ipv6on><ipmodev6>AUTO</
ipmodev6><ipaddresslinklocalv6></ipaddresslinklocalv6><ipaddressv6></ipaddressv6><gatewayv6></gatewayv6><submasklengthv6>0</submasklengthv6></IP></
param_set><param_set><ID><![CDATA[USB0]]></ID><ifenable>0</ifenable></param_set>BJNP.....BJNP.....SRC80;100;.....<pswdon>0,1</
pswdon><macfilteron>
</macfilteron><ipfilteron>
</ipfilteron><WSDon>0,1</WSDon><enableLAN>0,1</enableLAN><param_set><ID><![CDATA[wireless0]]></
ID><IP><ipmode>AUTOIP,DHCP,MANUAL</ipmode><ipv6on>0,1</ipv6on><ipmodev6>AUTO,MANUAL</ipmodev6></IP><802.11><wlmode>infra</
wlmode><ch>1,2,3,4,5,6,7,8,9,10,11,12,13</ch><wepon>0,1</wepon><wepid>1,2,3,4</wepid><weplength>64,128</weplength><auth>AUTO,OPEN,SHARED</
auth><wepformat>STRING,HEX</wepformat><pwrnmng>0,1</pwrnmng><wpaon>0,1</wpaon><wpamode>EAP/PSK</wpamode><wpa_encrypt>TKIP,CCMP</wpa_encrypt><wpa2on>0,1</
wpa2on><wpa2_encrypt>TKIP,CCMP</wpa2_encrypt></802.11></param_set><param_set><ID><![CDATA[USB0]]></ID><ifenable>0</ifenable></
param_set>.BJNP.....BJNP.....SRC80;100;.....BJNP.....BJNP.....
```

```
BJNP.....BJNP.....BJNP.....BJNP.....BJNP.....BJNP.....BJNP.....BJNP.....BJNP.....S
RC80;100;...u...<adminid>ADMIN</adminid><pswdon>1</pswdon><pswd>![CDATA[A[6978627a335133364b5578743251594b59386573]]</pswd><firmver>1.050</
firmver><firmUSBupdate>0</firmUSBupdate><firmLANupdate>0</firmLANupdate><enableLAN>1</enableLAN><param_set><ID>![CDATA[wireless0]]</ID><friendlyname></
macfilter><ipfilteron>0</ipfilteron><ipfilter></ipfilter><WSDon>1</WSDon><enableLAN>1</enableLAN><param_set><ID>![CDATA[wireless0]]</ID><friendlyname></
friendlyname><ifenable>1</ifenable><linkactive>1</linkactive><802.11><IFtype>n</IFtype><wlmode>infra</wlmode><ssid><[REDACTED]></
ssid><bssid>FFFFFFFFFFFF</bssid><ch>1</ch><wepon>0</wepon><weplength>64</weplength><wepformat>STRING</wepformat><auth>AUTO</auth><wepid>1</wepid><wep1></
wep1><wep2></wep2><wep3></wep3><wep4></wep4><wpaon>1</wpaon><wpamode>EAP/PSK</wpamode><wpa_encrypt>CCMP</wpa_encrypt><wpa2on>1</
wpa2on><wpa2_encrypt>CCMP</wpa2_encrypt><wpa_psk>757e602f782b32625278412b4a7a6131217a3d56</wpa_psk><setbssidenable>1</
setbssidenable><searchparamenable>1</searchparamenable></802.11><IP><ipmode>AUTO,MANUAL</ipmode><ipmodev6>192.168.
ipaddress><hwaddress><[REDACTED]></hwaddress><submask>255.255.255.0</submask><gateway>192.168.
ipmodev6><ipaddresslinklocalv6></ipaddresslinklocalv6><ipaddresssv6></ipaddresssv6><gatewayv6></gatewayv6><submasklengthv6>0</submasklengthv6></IP></
param_set><param_set><ID>![CDATA[USB0]]</ID><ifenable>0</ifenable></param_set>BJNP.....BJNP.....SRC80;100;.....<pswdon>0,1</
pswdon><macfilteron>0</macfilteron><ipfilteron>0</ipfilteron><WSDon>0,1</WSDon><enableLAN>0,1</enableLAN><param_set><ID>![CDATA[wireless0]]</
ID><IP><ipmode>AUTOIP,DHCP,MANUAL</ipmode><ipmodev6>0,1</ipmodev6><ipmodev6>AUTO,MANUAL</ipmodev6></IP><802.11><wlmode>infra</
wlmode><ch>1,2,3,4,5,6,7,8,9,10,11,12,13</ch><wepon>0,1</wepon><wepid>1,2,3,4</wepid><weplength>64,128</weplength><auth>AUTO,OPEN,SHARED</
auth><wepformat>STRING,HEX</wepformat><pwrnmng>0,1</pwrnmng><wpaon>0,1</wpaon><wpamode>EAP/PSK</wpamode><wpa_encrypt>TKIP,CCMP</wpa_encrypt><wpa2on>0,1</
wpa2on><wpa2_encrypt>TKIP,CCMP</wpa2_encrypt></802.11></param_set><param_set><ID>![CDATA[USB0]]</ID><ifenable>0</ifenable></
param_set>.BJNP.....BJNP.....SRC80;100;.....BJNP.....BJNP.....BJNP.....BJNP.....
```



```
>>> len("6978627a335133364b5578743251594b59386573")
40
>>> len("757e602f782b32625278412b4a7a6131217a3d56")
40
>>> █
```

Raw-SHA1 ?



Containing text:

pswd

Look in:

C:\Users\Fist0urs\Desktop\pwn_printer\pilotes\mp68-win-mg5200-1_05-ea24\mp68-win-mg5200-1_05-ea24\

Size (kB)

>

0






<

0

Modified:

After:

Today

| Name | Location | Size | Hits |
|---|---|----------|------|
|  IJLSX3.dll | C:\Users\Fist0urs\Desktop\pwn_printer\pilotes\mp6... \DrvSetup\ | 866 KB | 10 |
|  IJLSX6.dll | C:\Users\Fist0urs\Desktop\pwn_printer\pilotes\mp6... \DrvSetup\ | 1 023 KB | 10 |
|  CNMNPPM.DLL | C:\Users\Fist0urs\Desktop\pwn_printer\pilotes\mp68-win... \LAN\ | 358 KB | 2 |
|  CNMNPUTC.DLL | C:\Users\Fist0urs\Desktop\pwn_printer\pilotes\mp6... \NWTOOL\ | 979 KB | 4 |
|  CNMN6UTC.DLL | C:\Users\Fist0urs\Desktop\pwn_printer\pilotes\mp6... \NWTOOL\ | 1 043 KB | 4 |

f sub_10023190
f **DllEntryPoint**
f InitializePrintMonitor2
f sub_100233A5
f sub_100234A5
f sub_1002378A
f sub_100239AA
f sub_10023B2A
f sub_10024621
f sub_1002474E
f sub_100247E0
f sub_10024B65
f sub_10024DEE

| | | | | |
|---|----------------|----------|---|-----------|
| s | .text:100228C4 | 0000000A | C | macfilter |
| s | .text:100228D0 | 00000008 | C | extmode |
| s | .text:100228D8 | 00000008 | C | firmver |
| s | .text:100228E0 | 00000005 | C | pswd |
| s | .text:100228E8 | 00000008 | C | adminid |
| s | .text:100228F0 | 00000008 | C | gateway |
| s | .text:100228F8 | 00000008 | C | submask |
| s | .text:10022900 | 0000000A | C | hwaddress |
| s | .text:1002290C | 0000000A | C | ipaddress |
| s | .text:10022918 | 00000005 | C | wep4 |
| s | .text:10022920 | 00000005 | C | wep3 |
| s | .text:10022928 | 00000005 | C | wep2 |
| s | .text:10022930 | 00000005 | C | wep1 |

```
if ( *(_BYTE *)a3 & 2 )
{
    LOBYTE(Dst) = 0;
    sub_1004D9D0(a3 + 260, (char *)&Dst, 256);
    v76 = *a2;
    v5 = sub_1004E180(a1, &v76, 0, (int)"pswd", (int)&Dst, &v77);
    if ( v5 )
        return v5;
}
```

```
do
{
    if ( v5 >= a3 - 2 )
        break;
    v6 = sprintf(v4, "%02X", *(_BYTE *)v3++);
    v4 += v6;
    v5 += v6;
}
while ( *(_BYTE *)v3 );
```

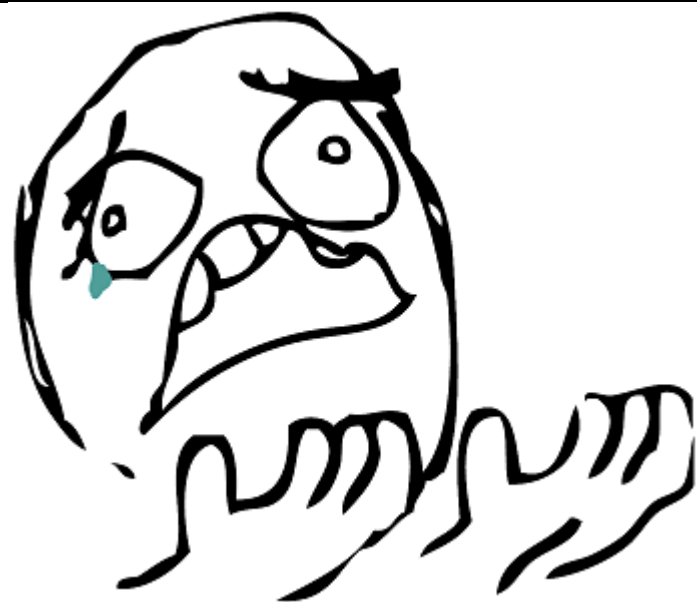


dafuq

```

>>> "6978627a335133364b5578743251594b59386573".decode("hex")
'ixbz3Q36KUxt2QYKY8es'
>>> "757e602f782b32625278412b4a7a6131217a3d56".decode("hex")
'u~`/x+2bRxA+Jza1!z=V'
>>> █

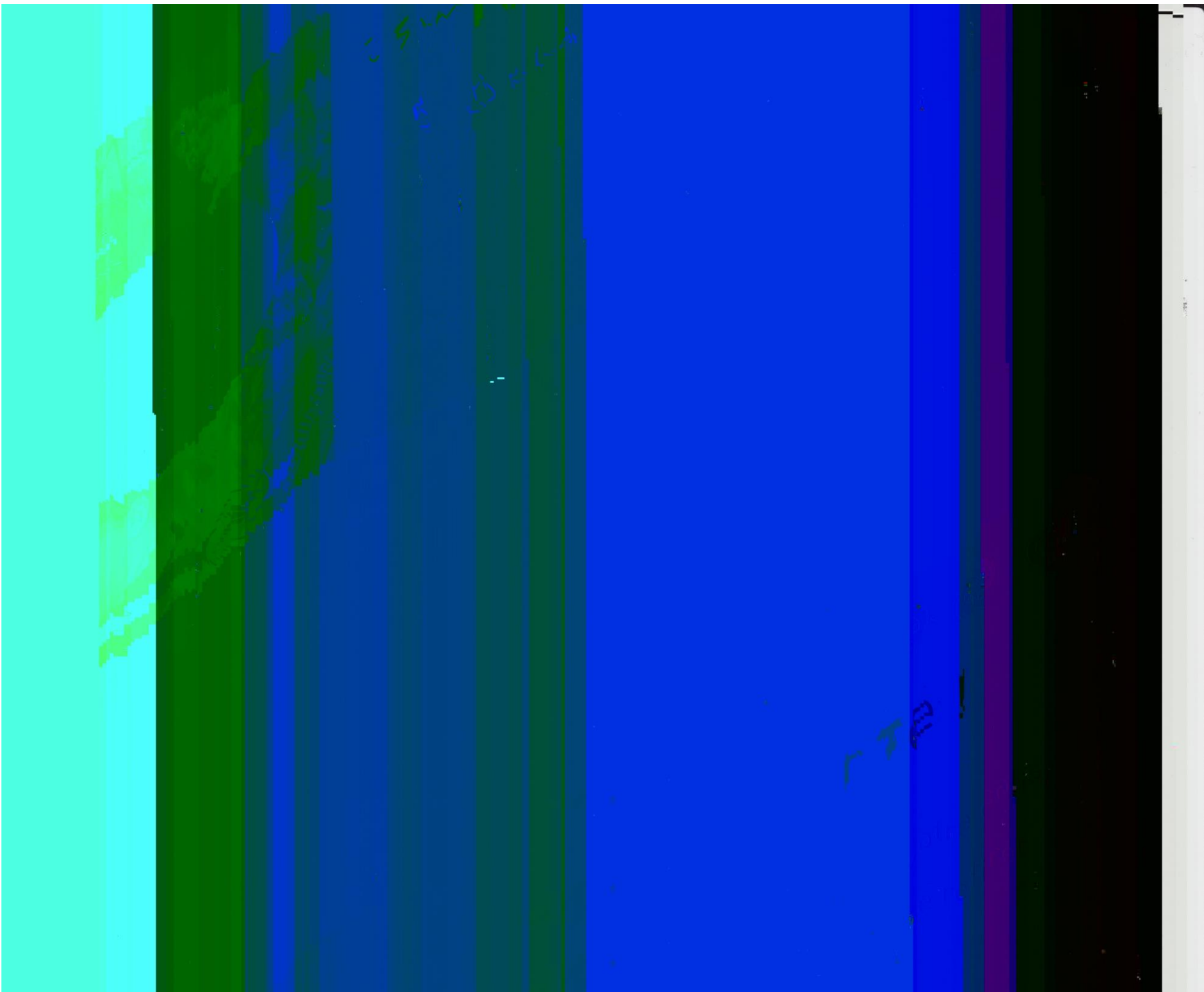
```



Conclusion :

- possibilité de récupérer le mot de passe de l'interface web d'administration de l'imprimante
- possibilité de récupérer le mot de passe de l'AP Wifi
- depuis un accès filaire...

```
~/Documents/Shared_Folder/pwn_printer$ hachoir-subfile fufu.pcapng  
[+] Start search on 5606264 bytes (5.3 MB)  
  
[+] File at 93506 size=305609 (298.4 KB): JPEG picture  
  
[+] End of search -- offset=5606264 (5.3 MB)  
Total time: 754 ms -- global rate: 7.1 MB/sec
```



[Calculated window size: 65535]

[Window size scaling factor: -2 (no window scaling used)]

▷ Checksum: 0xa00a [validation disabled]

Urgent pointer: 0

▷ [SEQ/ACK analysis]

TCP segment data (1460 bytes)

| | | | |
|------|-------------------------|-------------------------------|------------------|
| 0030 | ff ff a0 0a 00 00 | 42 4a 4e 50 82 20 00 00 00 8e |BJ NP. |
| 0040 | 00 3e 00 00 1f f0 06 06 | 00 00 00 00 00 00 00 00 | .>..... |
| 0050 | 00 00 00 00 40 00 ff d8 | ff e0 00 10 4a 46 49 46 |@... ..JFIF |
| 0060 | 00 01 02 01 02 58 02 58 | 00 00 ff db 00 84 00 04 |X.X |
| 0070 | 03 03 03 03 02 04 03 03 | 03 05 04 04 05 06 0b 07 | |
| 0080 | 06 06 06 06 0d 09 0a 08 | 0b 10 0e 11 10 0f 0e 0f | |
| 0090 | 0f 11 14 19 15 11 13 18 | 13 0f 0f 16 1e 16 18 1a | |
| 00a0 | 1b 1c 1d 1c 11 15 1f 21 | 1f 1c 21 19 1c 1c 1b 01 |! ..! |
| 00b0 | 04 05 05 06 05 06 0d 07 | 07 0d 1b 12 0f 12 1b 1b | |
| 00c0 | 1b 1b 1b 1b 1b 1b 1b 1b | 1b 1b 1b 1b 1b 1b 1b 1b | |
| 00d0 | 1b 1b 1b 1b 1b 1b 1b 1b | 1b 1b 1b 1b 1b 1b 1b 1b | |
| 00e0 | 1b 1b 1b 1b 1b 1b 1b 1b | 1b 1b 1b 1b 1b 1b 1b 1b | |
| 00f0 | ff c4 01 a2 00 00 01 05 | 01 01 01 01 01 01 00 00 | |



RECRUTE

