Assumptions

Adobe Connect is safe to run

...so I don't get 0wn3d

And provides confidentiality

- SSAC discussions
- RSSAC discussions
- Board discussions
- NOMCOM discussons

Time to question these assumptions...

Is anyone watching?

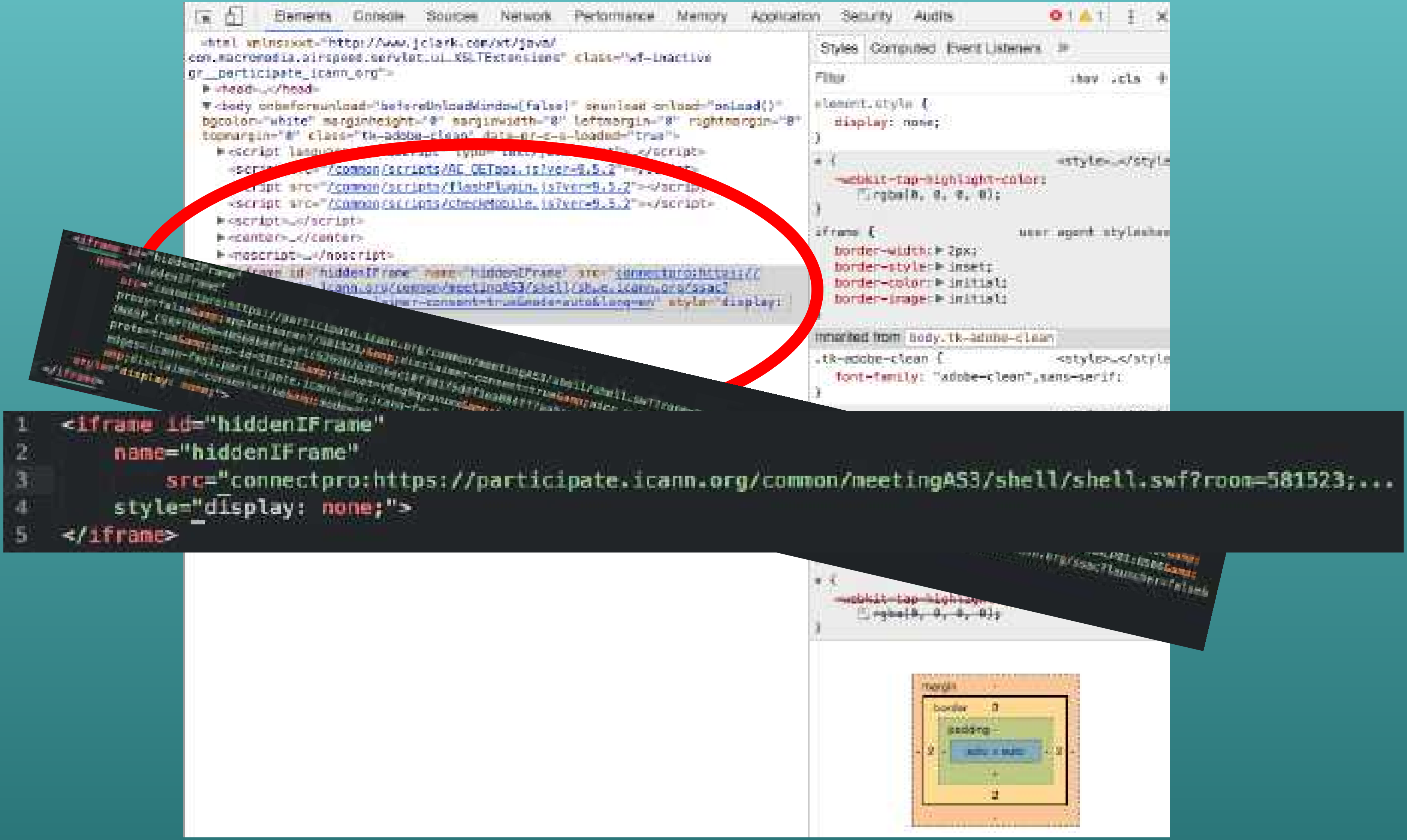
What's the problem?

We all use Adobe Connect to participate in ICANN
and follow links like: https://participate.icann.org/ssac
and then "magic" happens... but how?

I'd kind of been scared to look
... because Adobe
... and Flash
... but one day I was feeling brave,
... and had had my morning coffee
... and we'd been talking about confidentiality

Scared, but looking…

Where *is* the magic?



```
<html xmlns:xxt="http://www.jclark.com/xt/java/
com.macromedia.airspeed.servlet.ui.XSLTExtensions" class="wf-inactive
gr__participate_icann_org">
  ▶<head>…</head>
  ▼<body onbeforeunload="beforeUnloadWindow(false)" onunload onload="onload()"
  bgcolor="white" marginheight="0" marginwidth="0" leftmargin="0" rightmargin="0"
  topmargin="0" class="tk-adobe-clean" data-gr-c-s-loaded="true">
    ▶<script language=                type="text/                 ">…</script>
      <script          "/common/scripts/AC_OETags.js?ver=9.5.2"></script>
      <script src="/common/scripts/flashPlugin.js?ver=9.5.2"></script>
      <script src="/common/scripts/checkMobile.js?ver=9.5.2"></script>
    ▶<script>…</script>
    ▶<center>…</center>
    ▶<noscript>…</noscript>
      <iframe id="hiddenIFrame" name="hiddenIFrame" src="connectpro:https://
      …icann.org/common/meetingAS3/shell/sh…icann.org/ssac/
      …imer-consent=true&mode=auto&lang=en" style="display:
```

```
element.style {
  display: none;
}
* {                                        <style>…</style>
  -webkit-tap-highlight-color:
    rgba(0, 0, 0, 0);
}
iframe {                                   user agent stylesheet
  border-width: ▶ 2px;
  border-style: ▶ inset;
  border-color: ▶ initial;
  border-image: ▶ initial;
}
Inherited from body.tk-adobe-clean
.tk-adobe-clean {                          <style>…</style>
  font-family: "adobe-clean",sans-serif;
}
* {
  -webkit-tap-highlight-
    rgba(0, 0, 0, 0);
}
```

```
<iframe id="hiddenIFrame"
    name="hiddenIFrame"
        src="connectpro:https://participate.icann.org/common/meetingAS3/shell/shell.swf?room=581523;...
    style="display: none;">
</iframe>
```

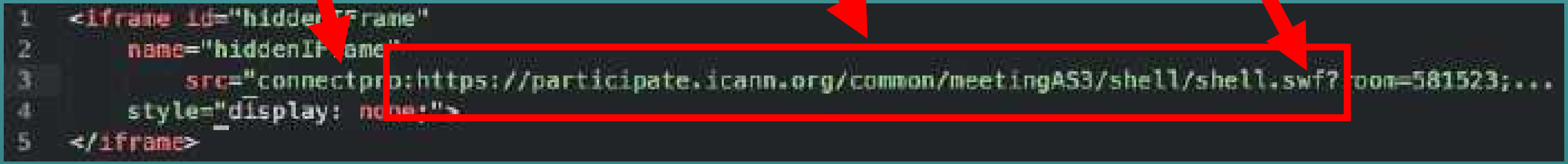
Break it down...

Thingie which invokes plugin.

.swf - ShockWave Flash?

Surely not...

URL



```
<iframe id="hiddenIFrame"
    name="hiddenIFrame"
        src="connectpro:https://participate.icann.org/common/meetingAS3/shell/shell.swf?room=581523;...
    style="display: none;">
</iframe>
```

What's the problem?

- Well that's odd, I've got the plugin, why does it make me get the .swf file?
- Surely the Adobe Connect Plugin is, well, Adobe Connect.
- Perhaps it's just the config?
  - Nope, it's ~300KB compressed
  - and contains images
- Let's see what the connectpro: handler is / does.
- `~/Library/Preferences/Macromedia/Flash\ Player//www.macromedia.com/bin/adobeconnectaddin/adobeconnectaddin.app/Contents/MacOS/adobeconnectaddin`
- I've got a *bad*, *bad* feeling about this...

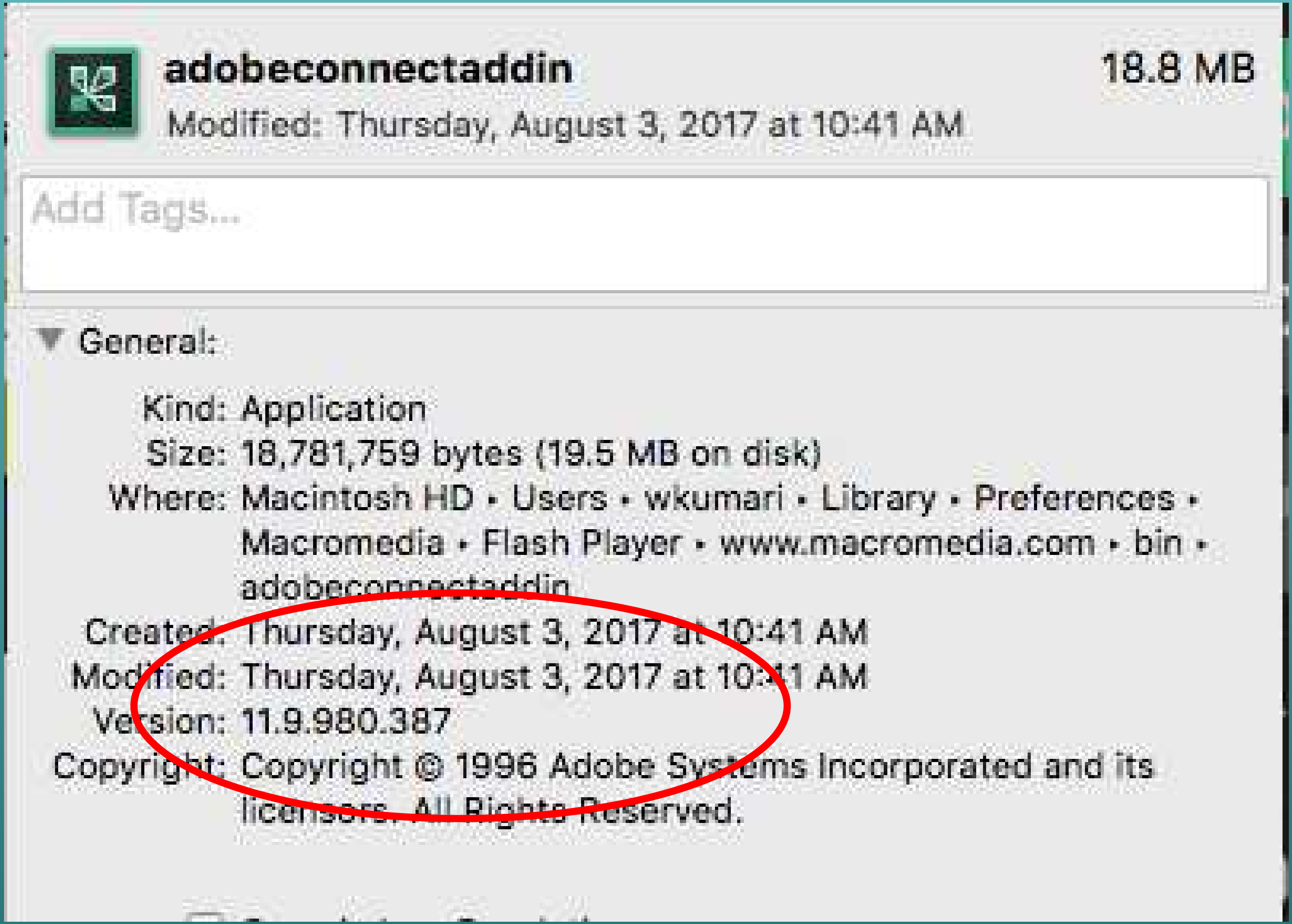
What's the problem?

- Let's give it another URL instead....
- https://af7.org/adobe.html

```
root@ron[0]:/var/
<html><body>
    <h1>Demo pag
    <meta http-e                                   .com/badger.swf">
    <a href="con                                  r badgers...</a>
</body></html>
```

What's the problem?

So, what is this thing?



adobeconnectaddin 18.8 MB

Modified: Thursday, August 3, 2017 at 10:41 AM

▼ General:

Kind: Application

Size: 18,781,759 bytes (19.5 MB on disk)

Where: Macintosh HD ▸ Users ▸ wkumari ▸ Library ▸ Preferences ▸ Macromedia ▸ Flash Player ▸ www.macromedia.com ▸ bin ▸ adobeconnectaddin

Created: Thursday, August 3, 2017 at 10:41 AM

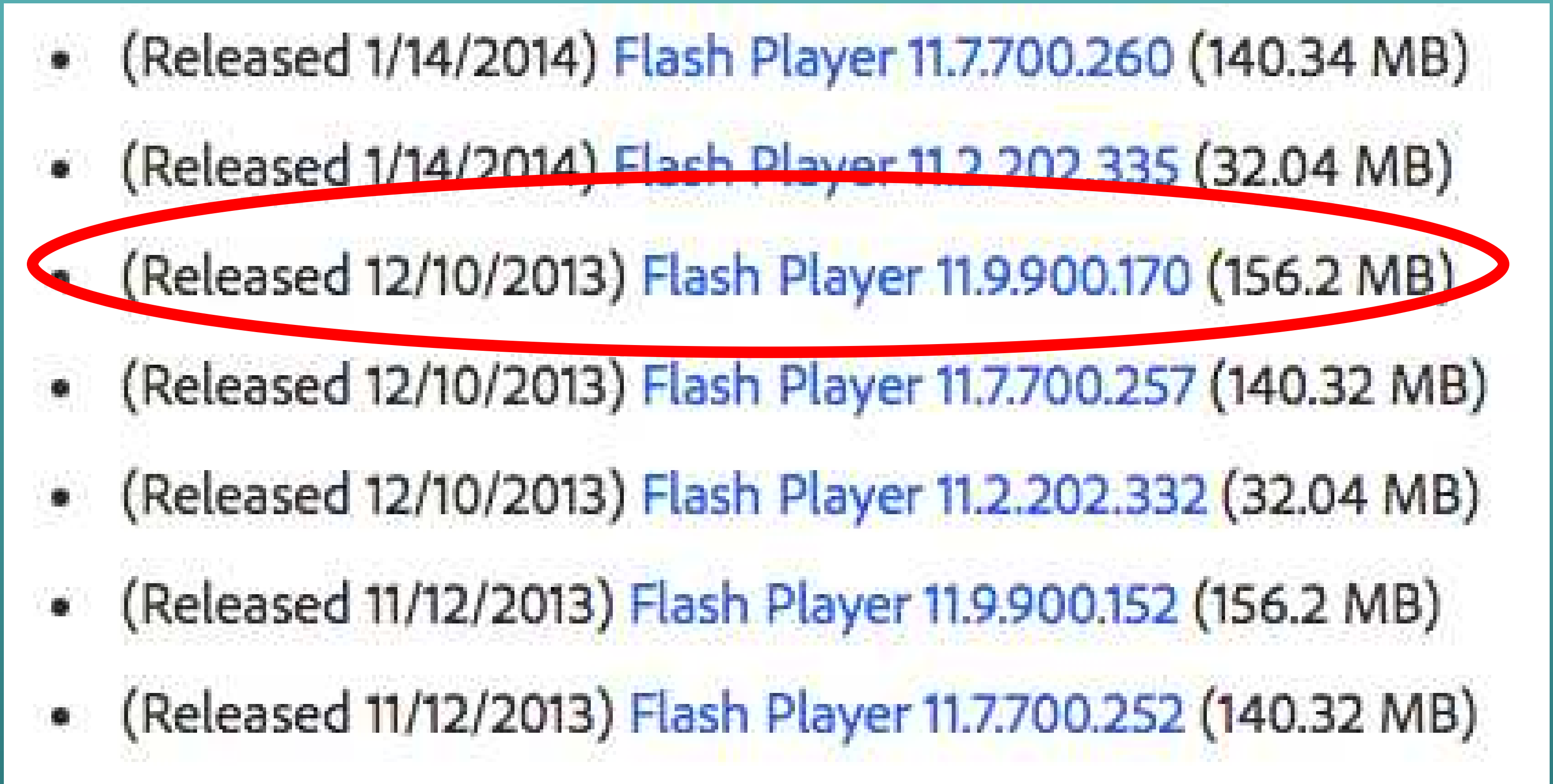
Modified: Thursday, August 3, 2017 at 10:41 AM

Version: 11.9.980.387

Copyright: Copyright © 1996 Adobe Systems Incorporated and its licensors. All Rights Reserved.

What's the problem?

From 2013...

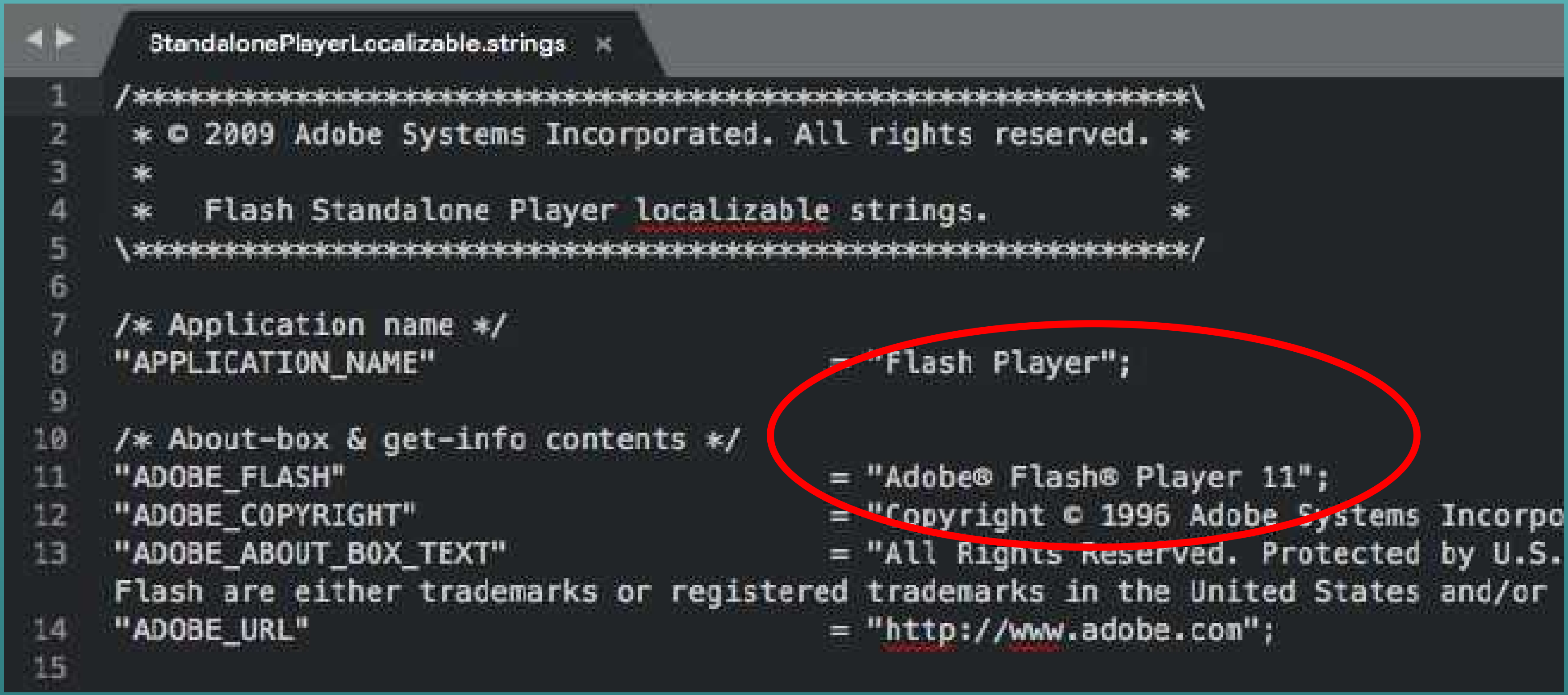


- (Released 1/14/2014) Flash Player 11.7.700.260 (140.34 MB)
- (Released 1/14/2014) Flash Player 11.2.202.335 (32.04 MB)
- (Released 12/10/2013) Flash Player 11.9.900.170 (156.2 MB)
- (Released 12/10/2013) Flash Player 11.7.700.257 (140.32 MB)
- (Released 12/10/2013) Flash Player 11.2.202.332 (32.04 MB)
- (Released 11/12/2013) Flash Player 11.9.900.152 (156.2 MB)
- (Released 11/12/2013) Flash Player 11.7.700.252 (140.32 MB)

Source: https://helpx.adobe.com/flash-player/kb/archived-flash-player-versions.html

What's the problem?

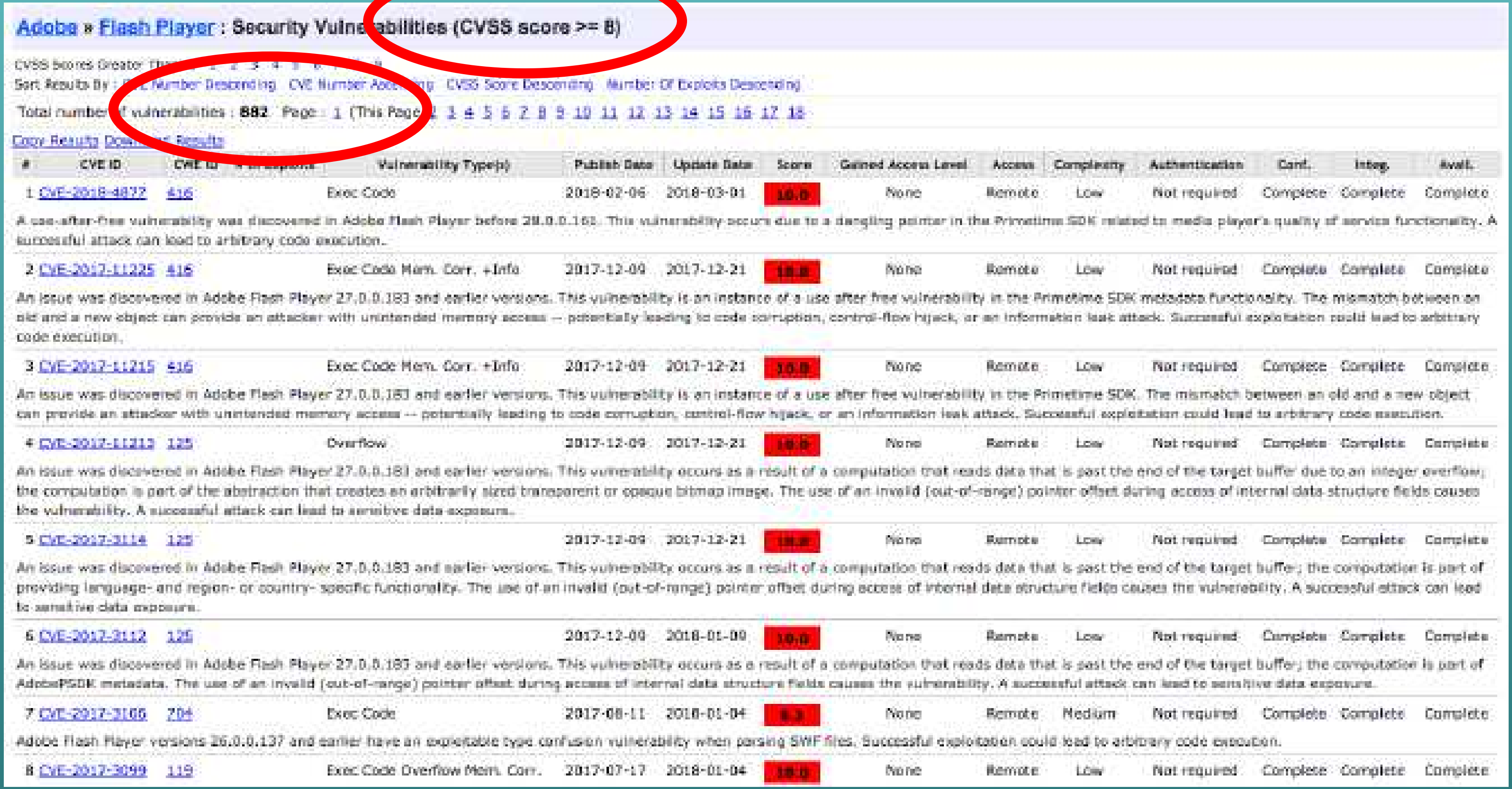
Surely not?



```
/******************************************************************\
 * © 2009 Adobe Systems Incorporated. All rights reserved. *
 *                                                         *
 *   Flash Standalone Player localizable strings.          *
\******************************************************************/

/* Application name */
"APPLICATION_NAME"                          = "Flash Player";

/* About-box & get-info contents */
"ADOBE_FLASH"                               = "Adobe® Flash® Player 11";
"ADOBE_COPYRIGHT"                           = "Copyright © 1996 Adobe Systems Incorpo
"ADOBE_ABOUT_BOX_TEXT"                      = "All Rights Reserved. Protected by U.S.
Flash are either trademarks or registered trademarks in the United States and/or
"ADOBE_URL"                                 = "http://www.adobe.com";

```

What's the problem?

Why should I care?



Adobe » Flash Player : Security Vulnerabilities (CVSS score >= 8)

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : 882 Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

Copy Results Download Results

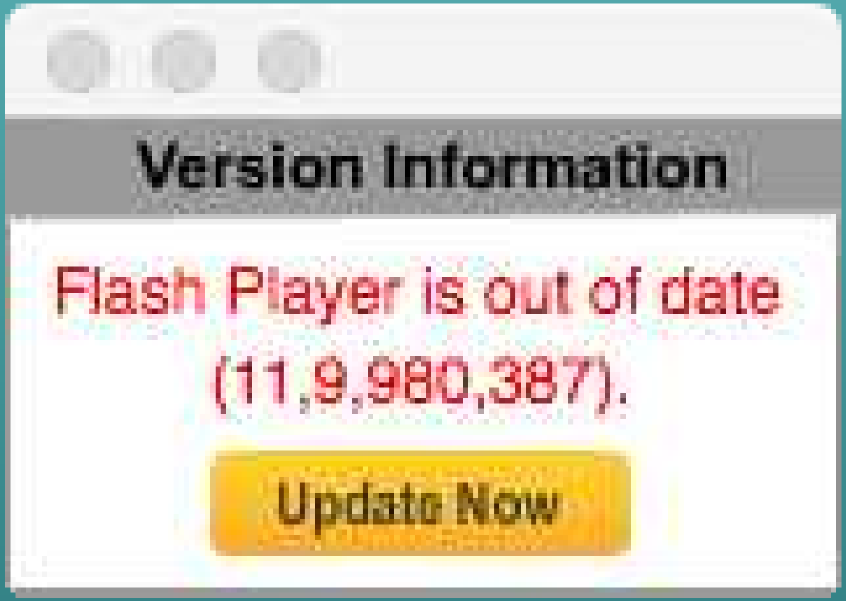
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-4877	416		Exec Code	2018-02-06	2018-03-01	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player's quality of service functionality. A successful attack can lead to arbitrary code execution.														
2	CVE-2017-11225	416		Exec Code Mem. Corr. +Info	2017-12-09	2017-12-21	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability is an instance of a use after free vulnerability in the Primetime SDK metadata functionality. The mismatch between an old and a new object can provide an attacker with unintended memory access -- potentially leading to code corruption, control-flow hijack, or an information leak attack. Successful exploitation could lead to arbitrary code execution.														
3	CVE-2017-11215	416		Exec Code Mem. Corr. +Info	2017-12-09	2017-12-21	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability is an instance of a use after free vulnerability in the Primetime SDK. The mismatch between an old and a new object can provide an attacker with unintended memory access -- potentially leading to code corruption, control-flow hijack, or an information leak attack. Successful exploitation could lead to arbitrary code execution.														
4	CVE-2017-11213	125		Overflow	2017-12-09	2017-12-21	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer due to an integer overflow; the computation is part of the abstraction that creates an arbitrarily sized transparent or opaque bitmap image. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.														
5	CVE-2017-3114	125			2017-12-09	2017-12-21	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of providing language- and region- or country- specific functionality. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.														
6	CVE-2017-3112	125			2017-12-09	2018-01-09	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of AdobePSDK metadata. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.														
7	CVE-2017-3106	704		Exec Code	2017-08-11	2018-01-04	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Adobe Flash Player versions 26.0.0.137 and earlier have an exploitable type confusion vulnerability when parsing SWF files. Successful exploitation could lead to arbitrary code execution.														
8	CVE-2017-3099	119		Exec Code Overflow Mem. Corr.	2017-07-17	2018-01-04	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

Source: https://www.cvedetails.com/vulnerability-list.php?vendor_id=53&product_id=6761

What's the problem?

- Perhaps the version is not really 11.9.xxx?
- Perhaps that's just the **plugin** version?!

http://af7.org/version.html



Version Information

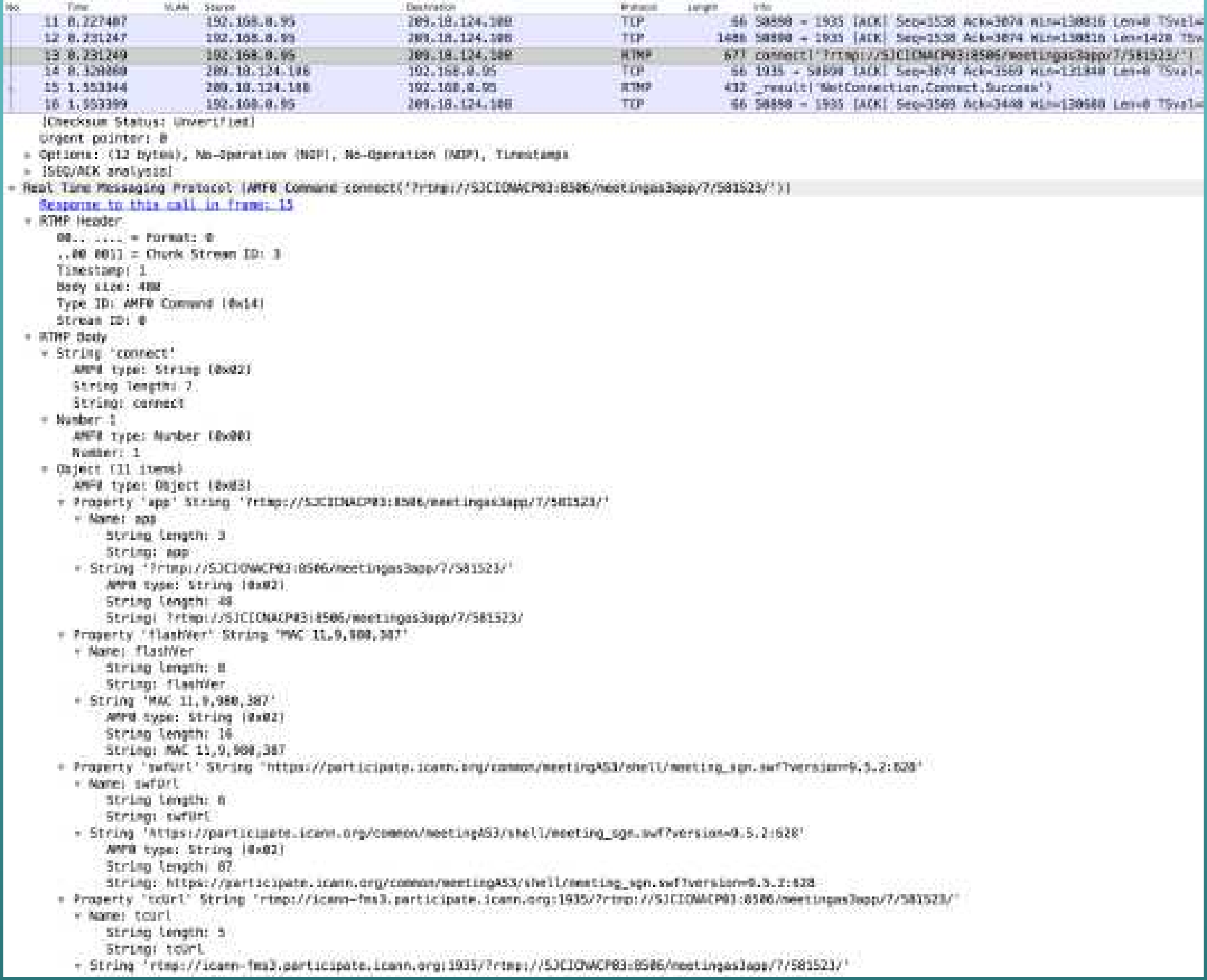
Flash Player is out of date (11,9,900,387).

Nope :-(

Source: http://owl-stretching-time.com/version.html

This makes me sad…

But wait! There's more!

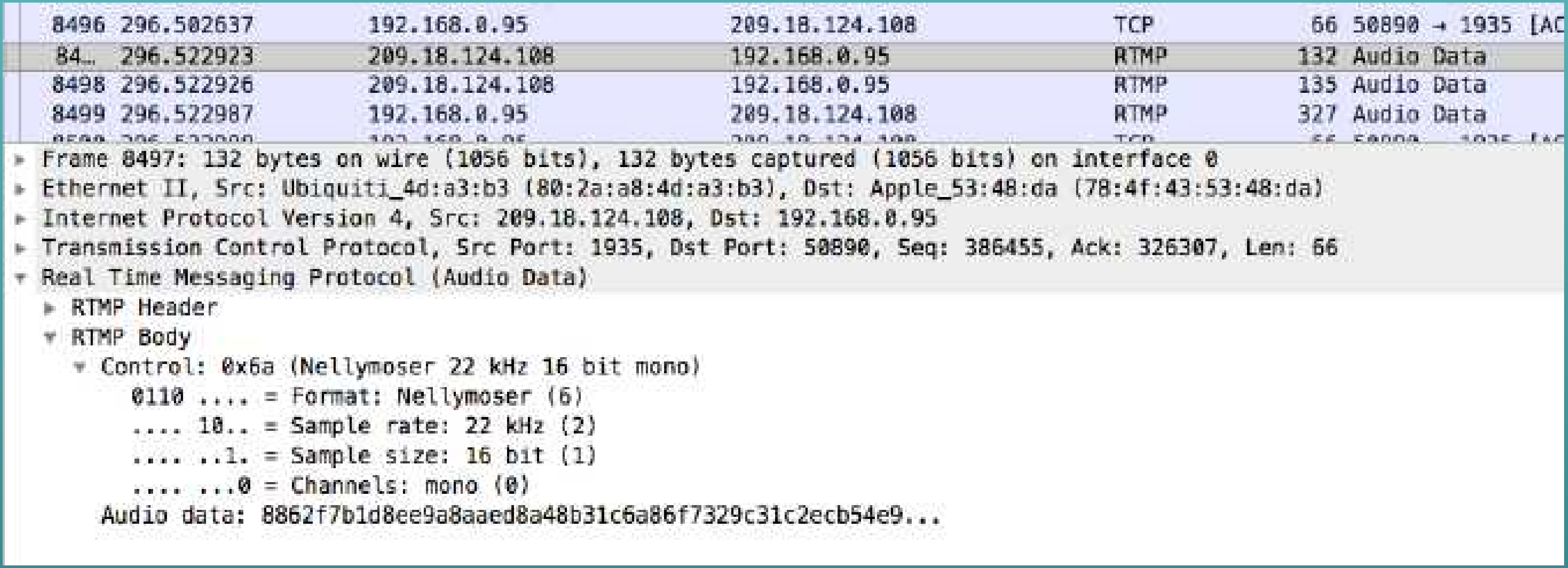


```
No.  Time       VLAN  Source            Destination       Protocol  Length  Info
  11 0.227407         192.168.0.95      209.18.124.100    TCP           66  50890 → 1935 [ACK] Seq=1538 Ack=3074 Win=130816 Len=0 TSval=
  12 0.231247         192.168.0.95      209.18.124.100    TCP         1486  50890 → 1935 [ACK] Seq=1538 Ack=3074 Win=130816 Len=1420 TSv
  13 0.231249         192.168.0.95      209.18.124.100    RTMP         677  connect('?rtmp://SJCICNACP03:8506/meetingas3app/7/581523/')
  14 0.320000         209.18.124.100    192.168.0.95      TCP           66  1935 → 50890 [ACK] Seq=3074 Ack=3569 Win=121840 Len=0 TSval=
  15 1.553344         209.18.124.100    192.168.0.95      RTMP         432  _result('NetConnection.Connect.Success')
  16 1.553399         192.168.0.95      209.18.124.100    TCP           66  50890 → 1935 [ACK] Seq=3569 Ack=3440 Win=130688 Len=0 TSval=
```

```
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
▾ Real Time Messaging Protocol (AMF0 Command connect('?rtmp://SJCICNACP03:8506/meetingas3app/7/581523/'))
    Response to this call in frame: 15
  ▾ RTMP Header
      00.. .... = Format: 0
      ..00 0011 = Chunk Stream ID: 3
      Timestamp: 1
      Body size: 400
      Type ID: AMF0 Command (0x14)
      Stream ID: 0
  ▾ RTMP Body
    ▾ String 'connect'
        AMF0 type: String (0x02)
        String length: 7
        String: connect
    ▾ Number 1
        AMF0 type: Number (0x00)
        Number: 1
    ▾ Object (11 items)
        AMF0 type: Object (0x03)
      ▾ Property 'app' String '?rtmp://SJCICNACP03:8506/meetingas3app/7/581523/'
        ▾ Name: app
            String length: 3
            String: app
        ▾ String '?rtmp://SJCICNACP03:8506/meetingas3app/7/581523/'
            AMF0 type: String (0x02)
            String length: 48
            String: ?rtmp://SJCICNACP03:8506/meetingas3app/7/581523/
      ▾ Property 'flashVer' String 'MAC 11,9,900,387'
        ▾ Name: flashVer
            String length: 8
            String: flashVer
        ▾ String 'MAC 11,9,900,387'
            AMF0 type: String (0x02)
            String length: 16
            String: MAC 11,9,900,387
      ▾ Property 'swfUrl' String 'https://participate.icann.org/common/meetingAS3/shell/meeting_sgn.swf?version=9.5.2:628'
        ▾ Name: swfUrl
            String length: 6
            String: swfUrl
        ▾ String 'https://participate.icann.org/common/meetingAS3/shell/meeting_sgn.swf?version=9.5.2:628'
            AMF0 type: String (0x02)
            String length: 87
            String: https://participate.icann.org/common/meetingAS3/shell/meeting_sgn.swf?version=9.5.2:628
      ▾ Property 'tcUrl' String 'rtmp://icann-fms3.participate.icann.org:1935/?rtmp://SJCICNACP03:8506/meetingas3app/7/581523/'
        ▾ Name: tcUrl
            String length: 5
            String: tcUrl
        ▾ String 'rtmp://icann-fms3.participate.icann.org:1935/?rtmp://SJCICNACP03:8506/meetingas3app/7/581523/'
```

But wait! There's more!

Unencrypted media...

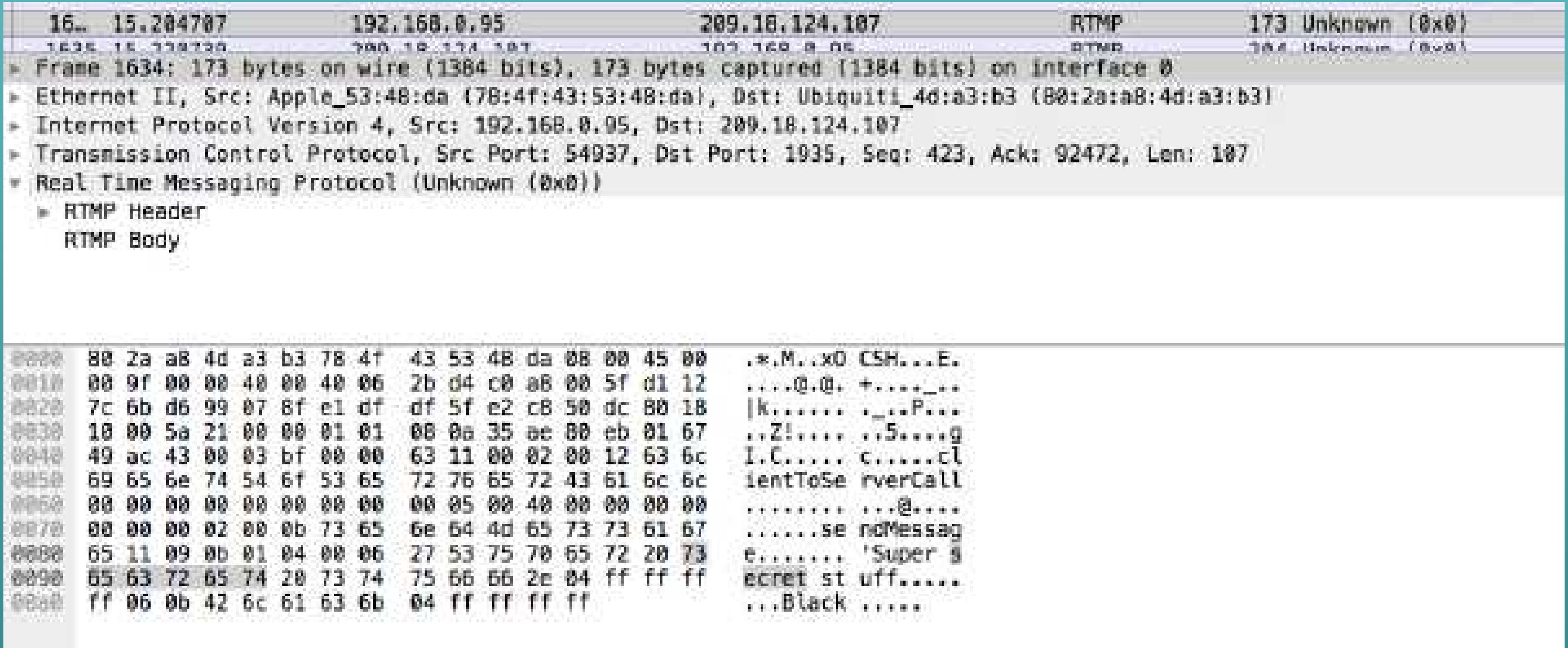


```
8496 296.502637   192.168.0.95     209.18.124.108   TCP    66 50890 → 1935 [AC
84…  296.522923   209.18.124.108   192.168.0.95     RTMP  132 Audio Data
8498 296.522926   209.18.124.108   192.168.0.95     RTMP  135 Audio Data
8499 296.522987   192.168.0.95     209.18.124.108   RTMP  327 Audio Data
▸ Frame 8497: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0
▸ Ethernet II, Src: Ubiquiti_4d:a3:b3 (80:2a:a8:4d:a3:b3), Dst: Apple_53:48:da (78:4f:43:53:48:da)
▸ Internet Protocol Version 4, Src: 209.18.124.108, Dst: 192.168.0.95
▸ Transmission Control Protocol, Src Port: 1935, Dst Port: 50890, Seq: 386455, Ack: 326307, Len: 66
▾ Real Time Messaging Protocol (Audio Data)
  ▸ RTMP Header
  ▾ RTMP Body
    ▾ Control: 0x6a (Nellymoser 22 kHz 16 bit mono)
        0110 .... = Format: Nellymoser (6)
        .... 10.. = Sample rate: 22 kHz (2)
        .... ..1. = Sample size: 16 bit (1)
        .... ...0 = Channels: mono (0)
      Audio data: 0862f7b1d8ee9a8aaed8a48b31c6a86f7329c31c2ecb54e9...
```

I munged the data around and kludged it into a codec - plays properly...

But wait! There's more!

… and chat!

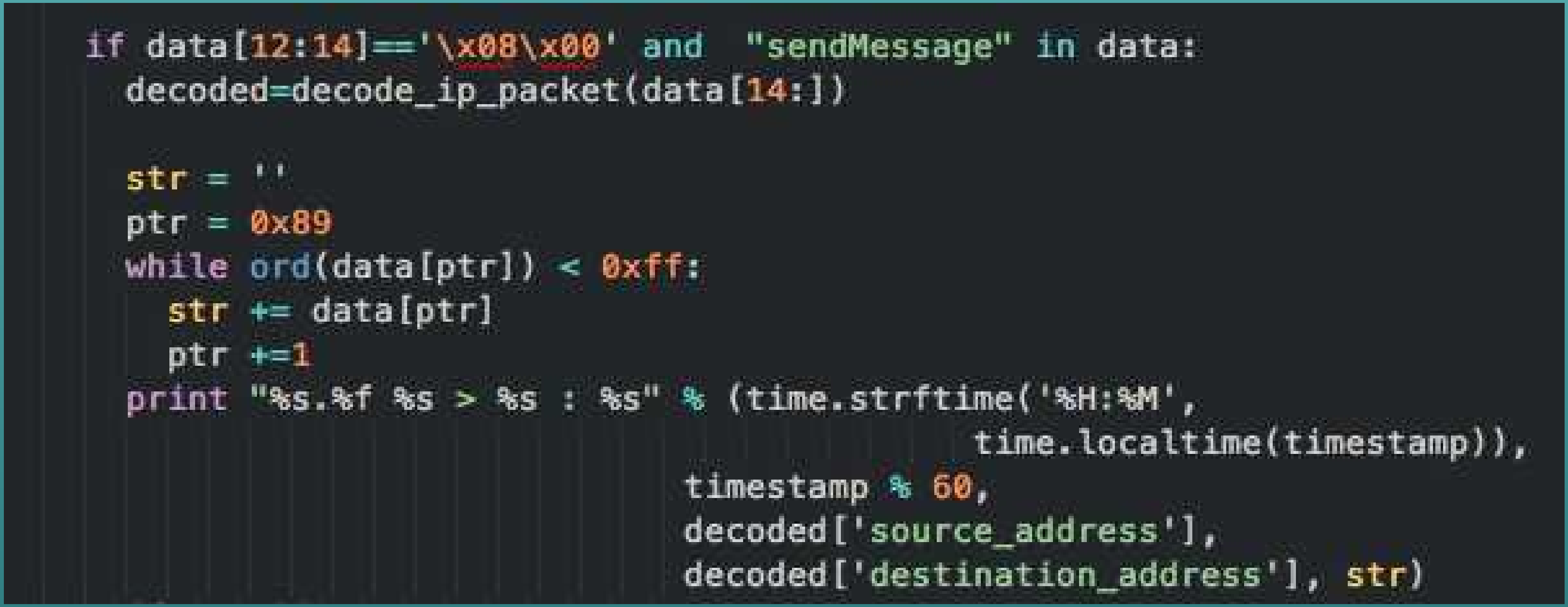


```
16…  15.204707   192.168.0.95     209.18.124.107   RTMP   173 Unknown (0x0)
1635 15.228728   209.18.124.107   192.168.0.95     RTMP   204 Unknown (0x0)
▸ Frame 1634: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface 0
▸ Ethernet II, Src: Apple_53:48:da (78:4f:43:53:48:da), Dst: Ubiquiti_4d:a3:b3 (80:2a:a8:4d:a3:b3)
▸ Internet Protocol Version 4, Src: 192.168.0.95, Dst: 209.18.124.107
▸ Transmission Control Protocol, Src Port: 54937, Dst Port: 1935, Seq: 423, Ack: 92472, Len: 107
▾ Real Time Messaging Protocol (Unknown (0x0))
   ▸ RTMP Header
     RTMP Body

0000  80 2a a8 4d a3 b3 78 4f  43 53 48 da 08 00 45 00   .*.M..xO CSH...E.
0010  00 9f 00 00 40 00 40 06  2b d4 c0 a8 00 5f d1 12   ....@.@. +...._..
0020  7c 6b d6 99 07 8f e1 df  df 5f e2 c8 50 dc 80 18   |k...... ._..P...
0030  10 00 5a 21 00 00 01 01  08 0a 35 ae 80 eb 01 67   ..Z!.... ..5....g
0040  49 ac 43 00 03 bf 00 00  63 11 00 02 00 12 63 6c   I.C..... c.....cl
0050  69 65 6e 74 54 6f 53 65  72 76 65 72 43 61 6c 6c   ientToSe rverCall
0060  00 00 00 00 00 00 00 00  00 05 00 40 00 00 00 00   ........ ...@....
0070  00 00 00 02 00 0b 73 65  6e 64 4d 65 73 73 61 67   ......se ndMessag
0080  65 11 09 0b 01 04 00 06  27 53 75 70 65 72 20 73   e....... 'Super s
0090  65 63 72 65 74 20 73 74  75 66 66 2e 04 ff ff ff   ecret st uff.....
00a0  ff 06 0b 42 6c 61 63 6b  04 ff ff ff ff            ...Black .....
```

Oooh! I've got an idea…

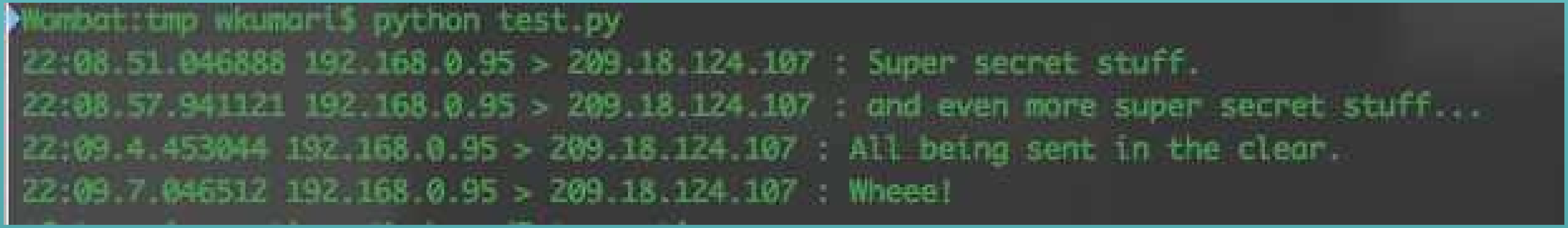
But wait! There's more!

Python with libpcap
... grab packets
... look for "sendMessage"
... and print the next bit



```
if data[12:14]=='\x08\x00' and  "sendMessage" in data:
  decoded=decode_ip_packet(data[14:])

  str = ''
  ptr = 0x89
  while ord(data[ptr]) < 0xff:
    str += data[ptr]
    ptr +=1
  print "%s.%f %s > %s : %s" % (time.strftime('%H:%M',
                                           time.localtime(timestamp)),
                             timestamp % 60,
                             decoded['source_address'],
                             decoded['destination_address'], str)
```

But wait! There's more!

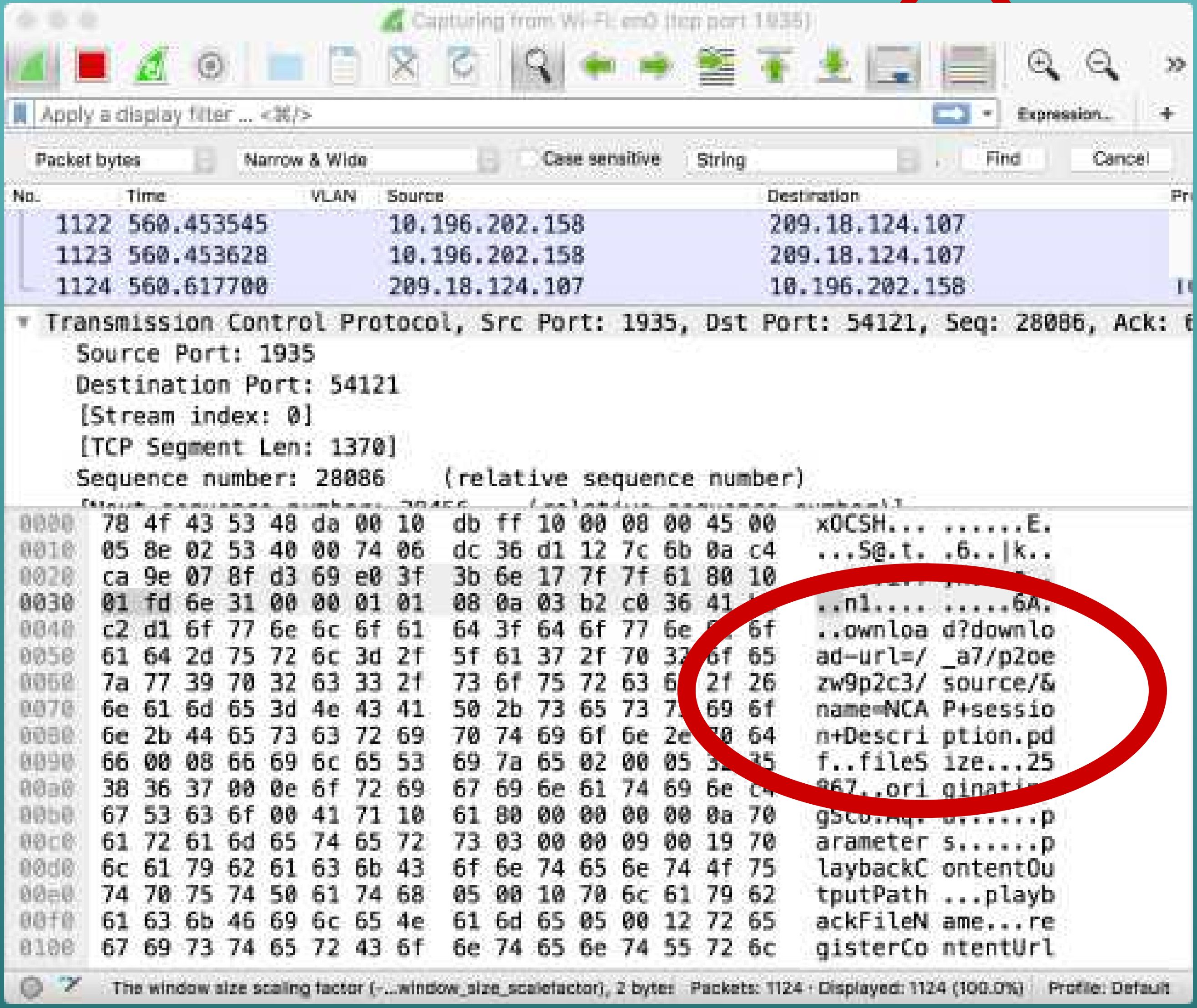


```
Wombat:tmp wkumari$ python test.py
22:08.51.046888 192.168.0.95 > 209.18.124.107 : Super secret stuff.
22:08.57.941121 192.168.0.95 > 209.18.124.107 : and even more super secret stuff...
22:09.4.453044 192.168.0.95 > 209.18.124.107 : All being sent in the clear.
22:09.7.046512 192.168.0.95 > 209.18.124.107 : Wheee!
```

This makes me more sad

even

But wait! There's more!



Capturing from Wi-Fi: en0 (tcp port 1935)
Apply a display filter … <⌘/>
Expression…
+
Packet bytes
Narrow & Wide
Case sensitive
String
Find
Cancel

```
No.    Time        VLAN  Source           Destination       Pr
  1122 560.453545        10.196.202.158   209.18.124.107
  1123 560.453628        10.196.202.158   209.18.124.107
  1124 560.617700        209.18.124.107   10.196.202.158    T(
```

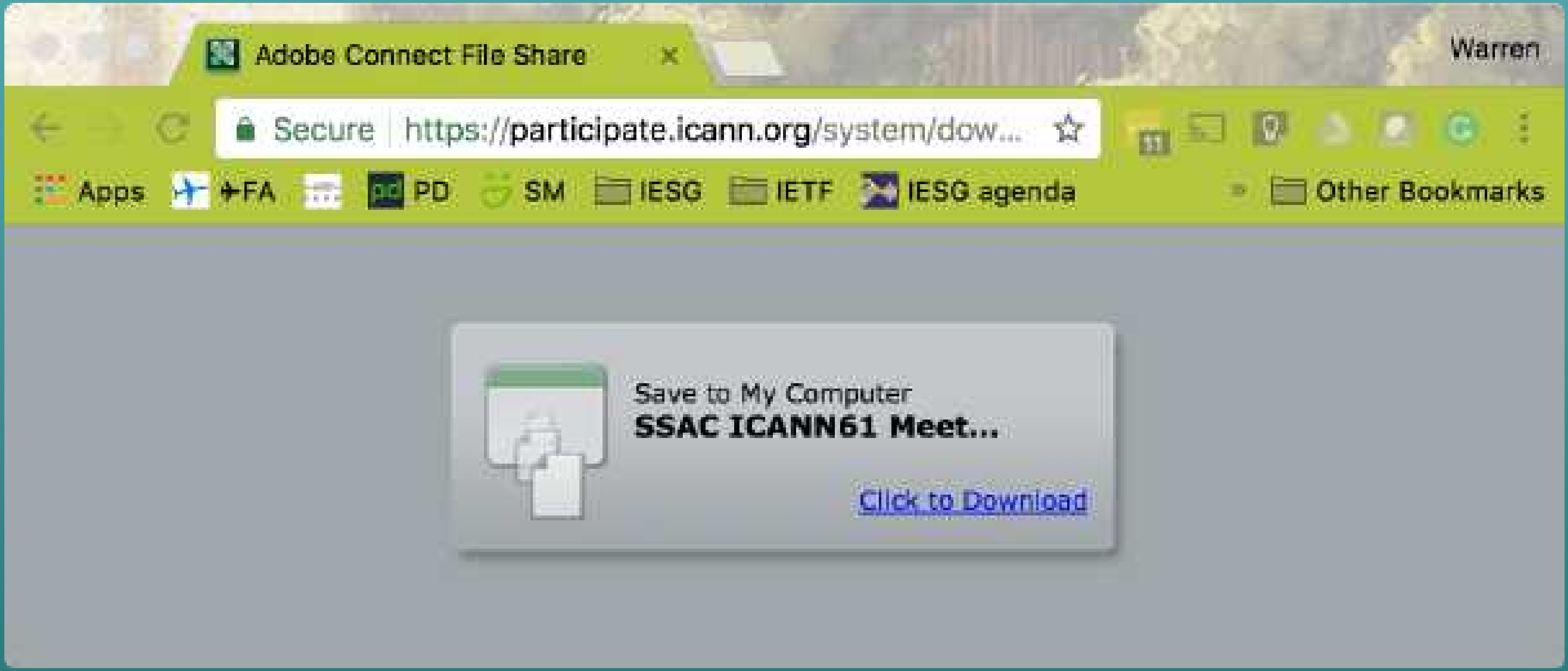
```
▼ Transmission Control Protocol, Src Port: 1935, Dst Port: 54121, Seq: 28086, Ack: 6
    Source Port: 1935
    Destination Port: 54121
    [Stream index: 0]
    [TCP Segment Len: 1370]
    Sequence number: 28086    (relative sequence number)
    [Next sequence number: 29456    (relative sequence number)]
```

```
0000  78 4f 43 53 48 da 00 10  db ff 10 00 08 00 45 00   xOCSH... ......E.
0010  05 8e 02 53 40 00 74 06  dc 36 d1 12 7c 6b 0a c4   ...S@.t. .6..|k..
0020  ca 9e 07 8f d3 69 e0 3f  3b 6e 17 7f 7f 61 80 10   .....i.? ;n...a..
0030  01 fd 6e 31 00 00 01 01  08 0a 03 b2 c0 36 41 2e   ..n1.... .....6A.
0040  c2 d1 6f 77 6e 6c 6f 61  64 3f 64 6f 77 6e 6c 6f   ..ownloa d?downlo
0050  61 64 2d 75 72 6c 3d 2f  5f 61 37 2f 70 32 6f 65   ad-url=/ _a7/p2oe
0060  7a 77 39 70 32 63 33 2f  73 6f 75 72 63 65 2f 26   zw9p2c3/ source/&
0070  6e 61 6d 65 3d 4e 43 41  50 2b 73 65 73 73 69 6f   name=NCA P+sessio
0080  6e 2b 44 65 73 63 72 69  70 74 69 6f 6e 2e 70 64   n+Descri ption.pd
0090  66 00 08 66 69 6c 65 53  69 7a 65 02 00 05 32 35   f..fileS ize...25
00a0  38 36 37 00 0e 6f 72 69  67 69 6e 61 74 69 6e 67   867..ori ginating
00b0  67 53 63 6f 00 41 71 10  61 80 00 00 00 00 0a 70   gSco.Aq. a......p
00c0  61 72 61 6d 65 74 65 72  73 03 00 00 09 00 19 70   arameter s......p
00d0  6c 61 79 62 61 63 6b 43  6f 6e 74 65 6e 74 4f 75   laybackC ontentOu
00e0  74 70 75 74 50 61 74 68  05 00 10 70 6c 61 79 62   tputPath ...playb
00f0  61 63 6b 46 69 6c 65 4e  61 6d 65 05 00 12 72 65   ackFileN ame...re
0100  67 69 73 74 65 72 43 6f  6e 74 65 6e 74 55 72 6c   gisterCo ntentUrl
```

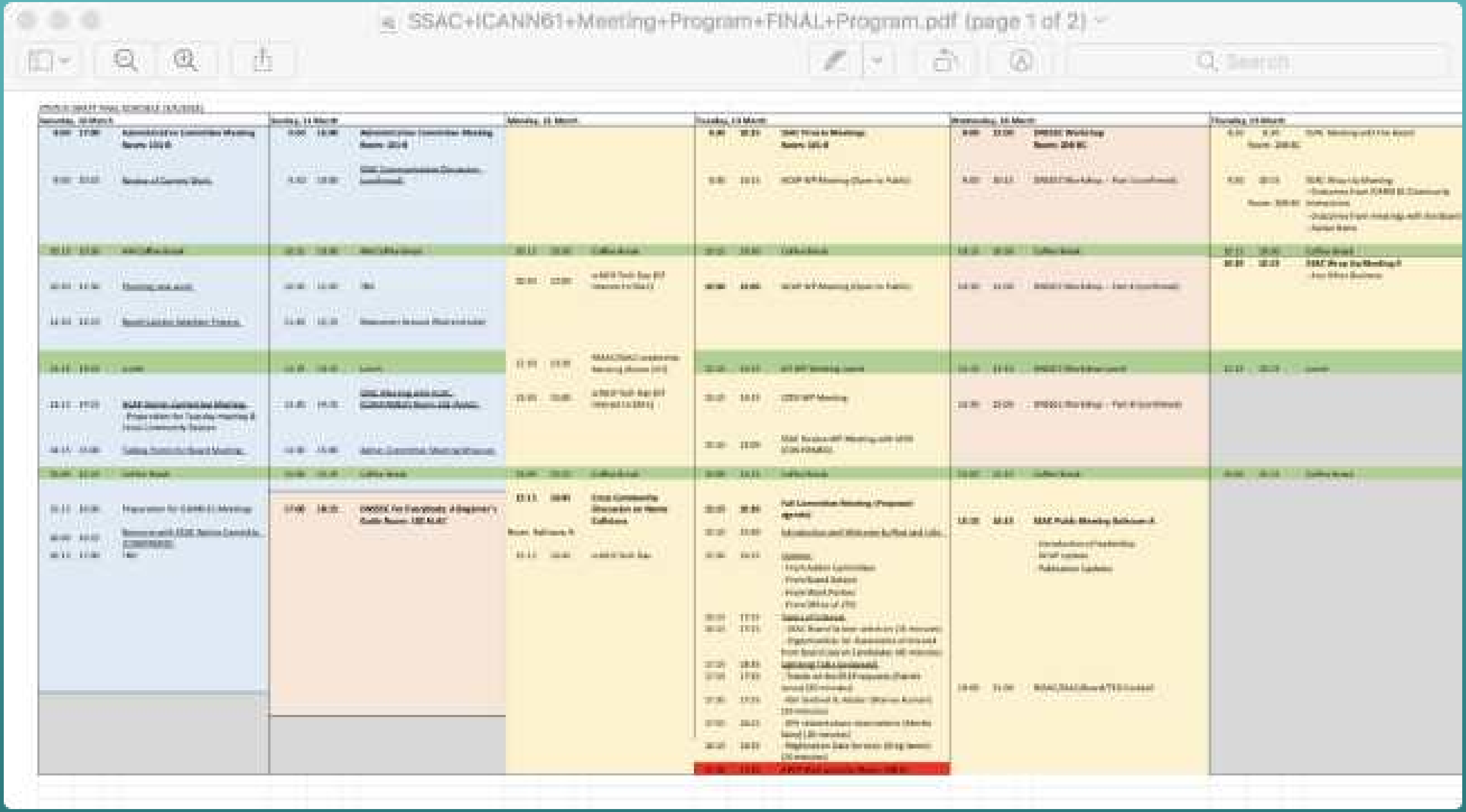
The window size scaling factor (-…window_size_scalefactor), 2 bytes   Packets: 1124 · Displayed: 1124 (100.0%)   Profile: Default

But wait! There's even more!

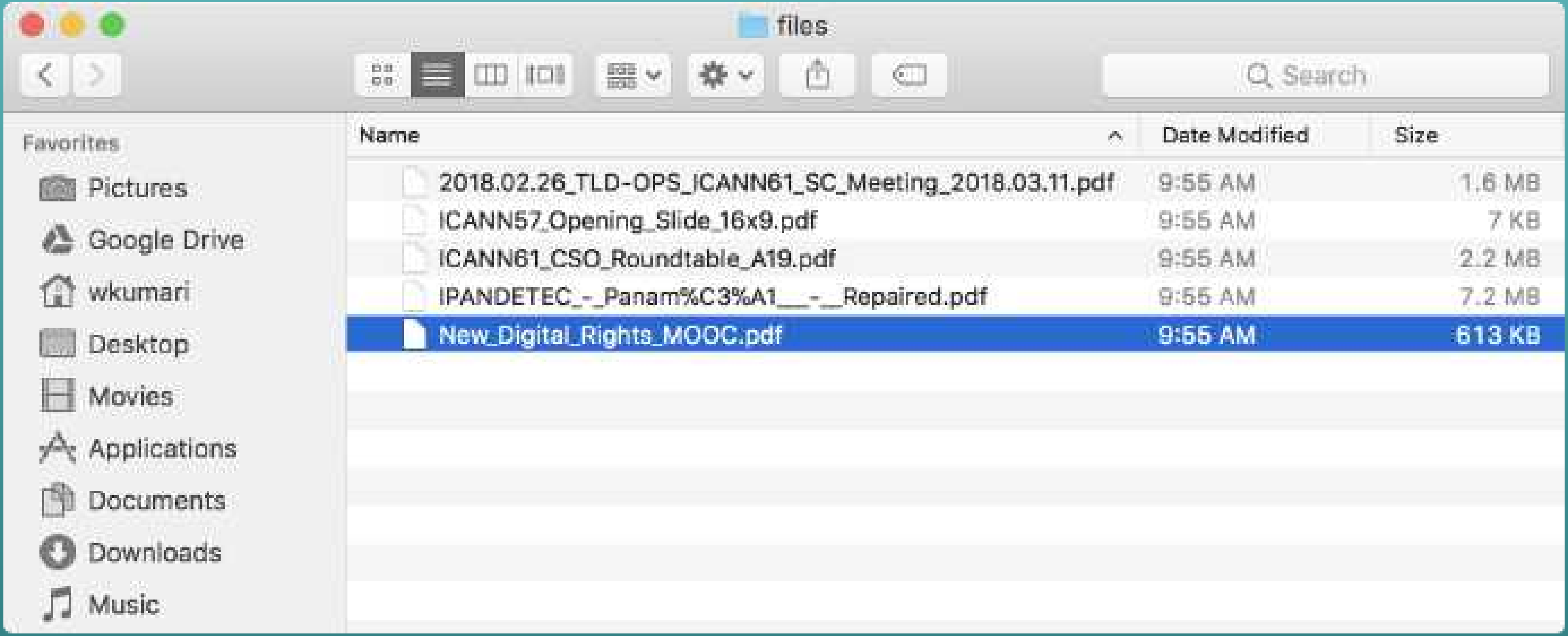
customDatadownloadUrl=/system/download?download-url=/_a7/p5acn81mat9/source/&name=SSAC+ICANN61+Meeting+Program+FINAL+Program.pdffile   Size79486



But wait! There's even more!


SSAC+ICANN61+Meeting+Program+FINAL+Program.pdf (page 1 of 2)
Search

But wait! There's even more!



Name	Date Modified	Size
2018.02.26_TLD-OPS_ICANN61_SC_Meeting_2018.03.11.pdf	9:55 AM	1.6 MB
ICANN57_Opening_Slide_16x9.pdf	9:55 AM	7 KB
ICANN61_CSO_Roundtable_A19.pdf	9:55 AM	2.2 MB
IPANDETEC_-_Panam%C3%A1__-_Repaired.pdf	9:55 AM	7.2 MB
New_Digital_Rights_MOOC.pdf	9:55 AM	613 KB

Questions?