WIFI MESHUP (PART UN)
WIFI @ 30K FEET
THE WRAP-UP

LUIZ "EFFFFN" EDUARDO

THOTCON 2010

WHO AM I IN 17 SECONDS

- G33K
- WORK
- INVOLVED WITH YOUR FAVORITE HACKER CON NETWORK
  - DEFCON
  - SHMOOCON
- AND... (SHAMELESS PLUG-IN)

MAY 17TH, 2010

AGENDA

- QUICK RECAP
- WHAT'S "NEW" W/ THE SERVICE SINCE DC17
- NEW THINGS I TRIED & OBSERVED
- WRAP-UP
- NELSON

Quick Recap (I promise)

- Presented this @
  - Toorcon San Diego 2008
  - GTS 12
  - Defcon 17
  - This is the wrap-up (maybe)
- Motivation
- The Basics
  - APs inside the plane
  - Service
  - The "magic" (Air to Ground communication)

INFLIGHT WIFI, SO WHAT?

- EXACTLY, JUST A BIG-ASS FLYING HOTSPOT
- FOR THE BASICS, LIKE:
  - # OF APS
  - FAA RANT
  - AIR-GROUND (BASIC) INFO
  - GROUND BACKBONE (BASIC) INFO
  - AIRLINES AND SERVICES DIFFERENCES

HTTP://WWW.VIMEO.COM/6310311

(STANDARD) HOTSPOT WIFI-(IN)SECURITY

Caffè Hours
Sun. 6:30am - 10:00 pm
Mon. 6:30am - 10:00 pm
Tue. 6:30am - 10:00 pm
Wed. 6:30am - 10:30 pm
Thur 6:30am - 10:00 pm
Fri. 6:30am - 12:00 pm
Sat. 6:30am - 12:00

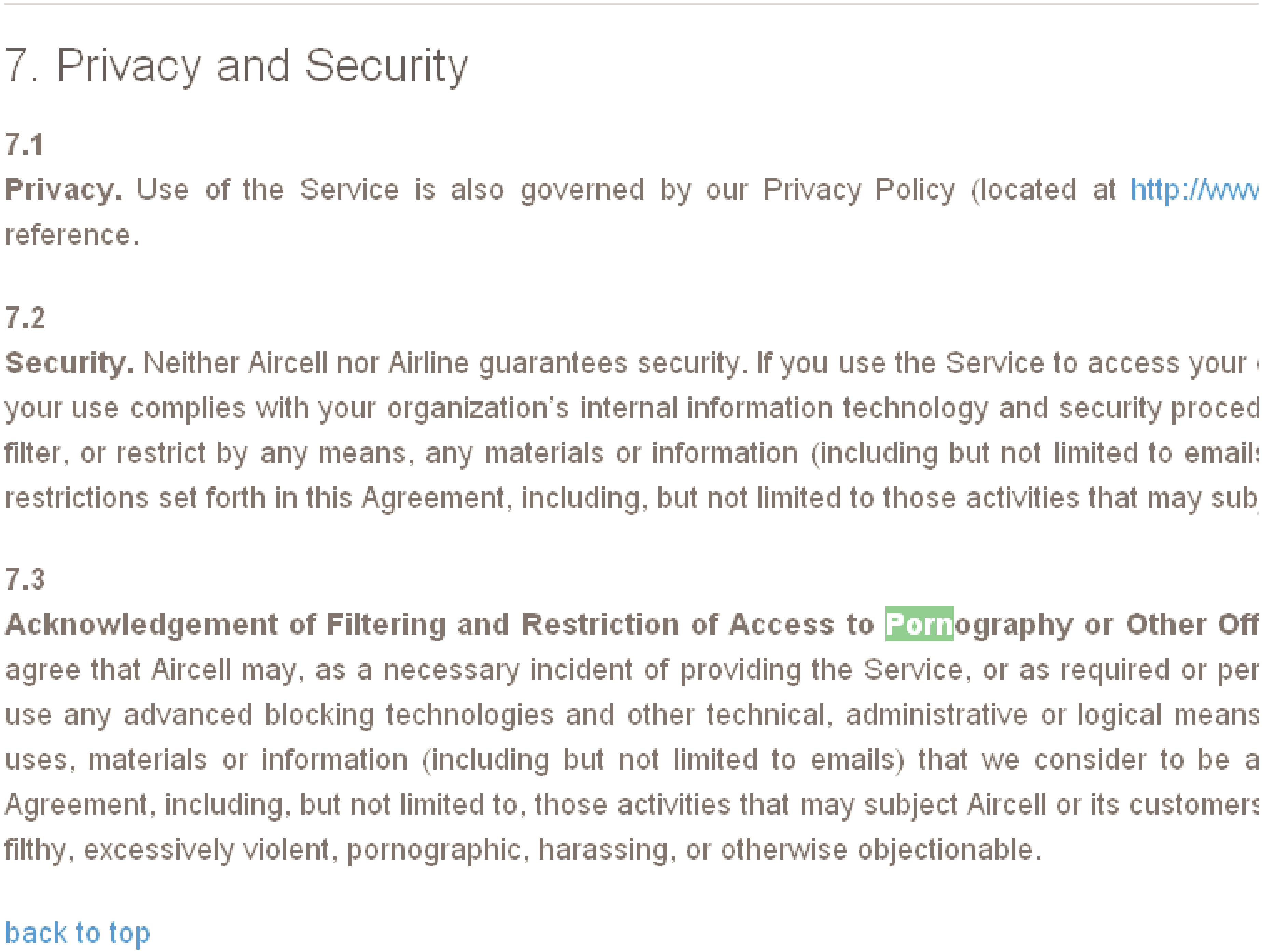
POST DEFCON 17

Celebrity Rehab

Not a single Celebrity, just rehab.

WHAT'S "NEW"?

- MORE FLIGHTS = BORED
- HOTSPOT SERVICE
- SSIDS
- ENUMERATION
  - DEVICES
  - PEOPLE
  - APPS
  - (ALL OF THE ABOVE TOGETHER)
- GROUND NETWORK ☹
- COOL SH1T / FUNNY STORIES



7. Privacy and Security

7.1

Privacy. Use of the Service is also governed by our Privacy Policy (located at http://www
reference.

7.2

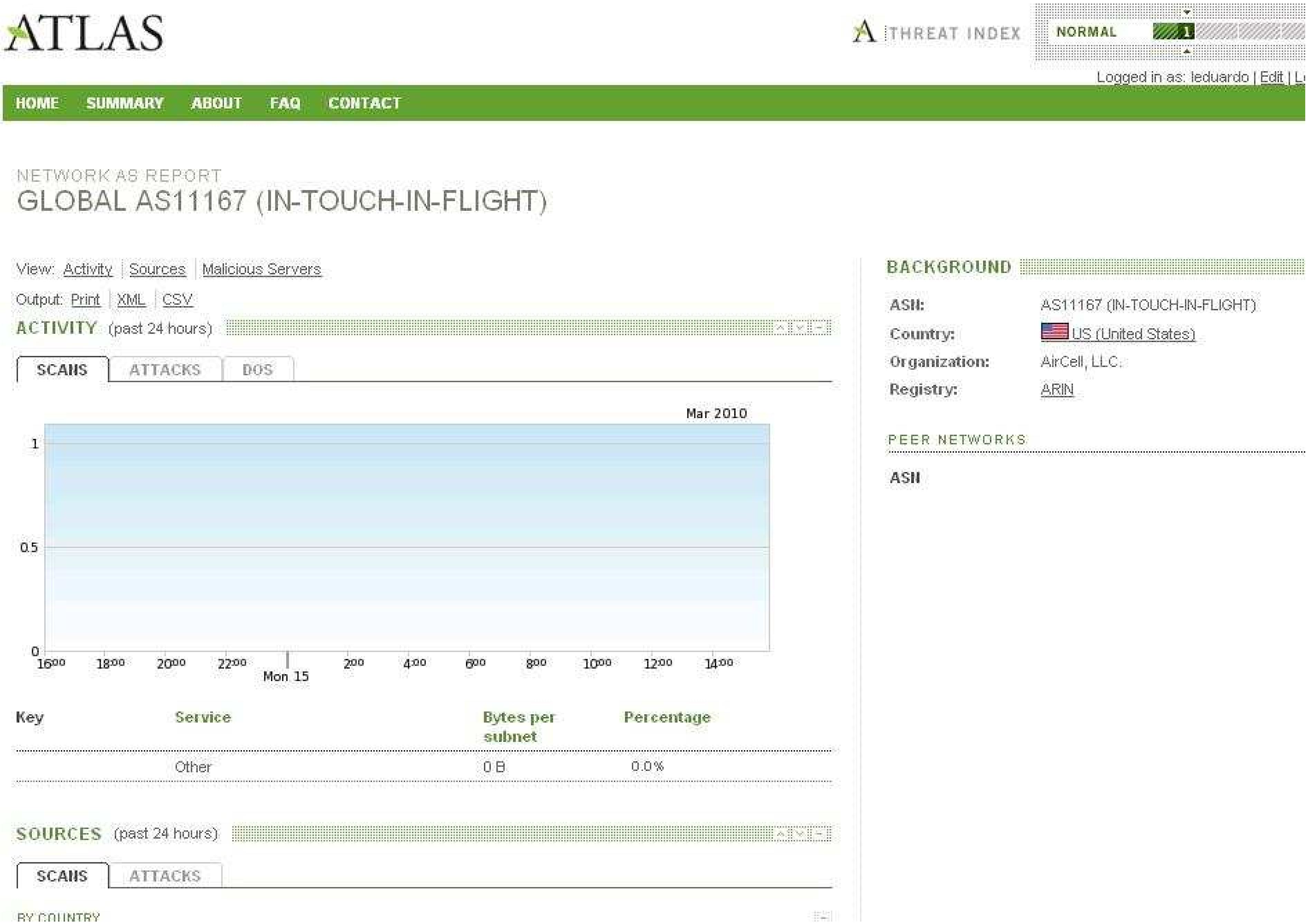
Security. Neither Aircell nor Airline guarantees security. If you use the Service to access your
your use complies with your organization's internal information technology and security proced
filter, or restrict by any means, any materials or information (including but not limited to email
restrictions set forth in this Agreement, including, but not limited to those activities that may sub

7.3

Acknowledgement of Filtering and Restriction of Access to Pornography or Other Off
agree that Aircell may, as a necessary incident of providing the Service, or as required or per
use any advanced blocking technologies and other technical, administrative or logical means
uses, materials or information (including but not limited to emails) that we consider to be a
Agreement, including, but not limited to, those activities that may subject Aircell or its customers
filthy, excessively violent, pornographic, harassing, or otherwise objectionable.

back to top

AIR TO GROUND



ATLAS

THREAT INDEX NORMAL 1

Logged in as: leduardo | Edit | L

HOME SUMMARY ABOUT FAQ CONTACT

NETWORK AS REPORT

GLOBAL AS11167 (IN-TOUCH-IN-FLIGHT)

View: Activity | Sources | Malicious Servers

Output: Print | XML | CSV

ACTIVITY (past 24 hours)

SCANS ATTACKS DOS

Key	Service	Bytes per subnet	Percentage
	Other	0 B	0.0%

SOURCES (past 24 hours)

SCANS ATTACKS

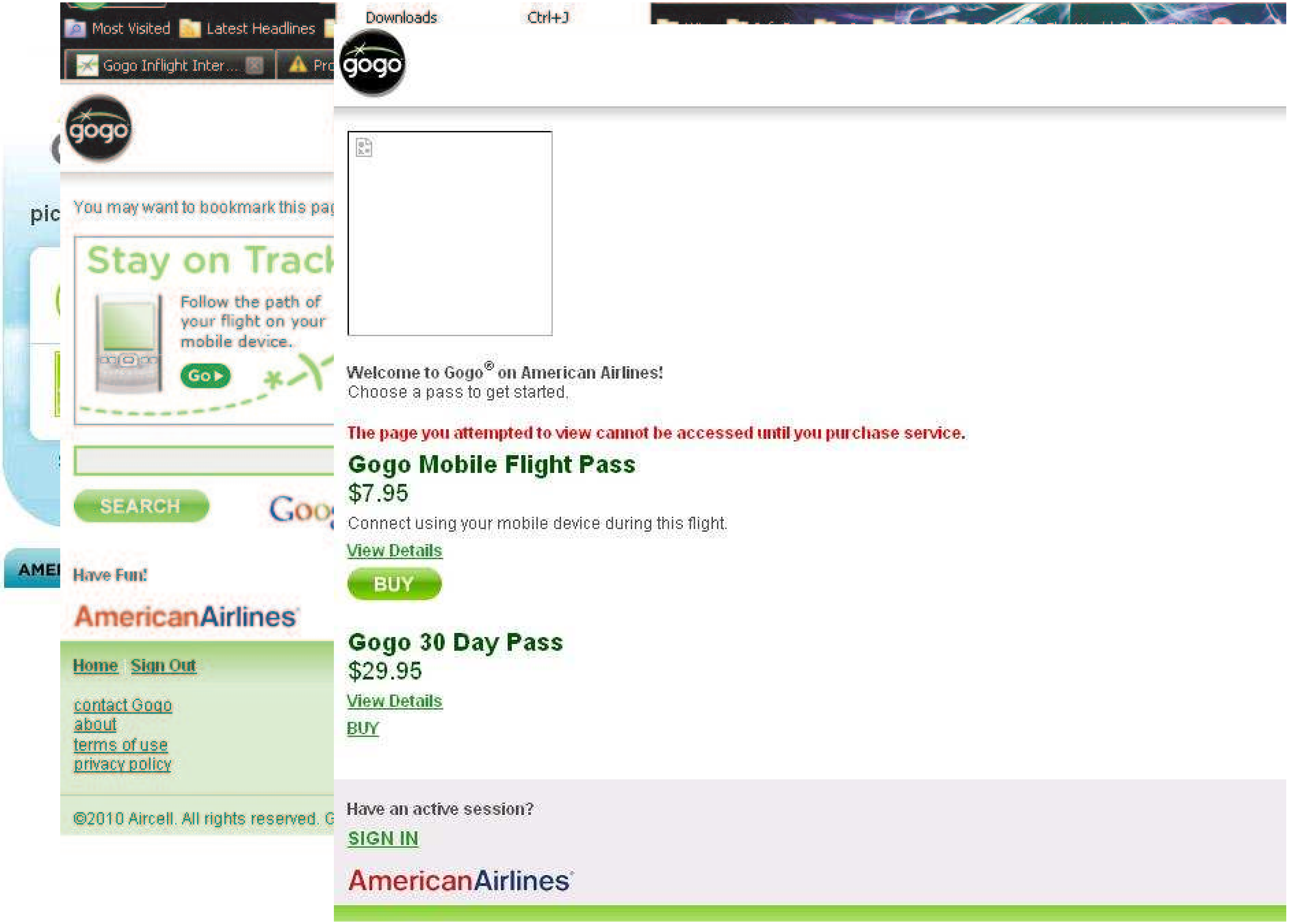
BY COUNTRY

BACKGROUND

ASN:	AS11167 (IN-TOUCH-IN-FLIGHT)
Country:	US (United States)
Organization:	AirCell, LLC.
Registry:	ARIN

PEER NETWORKS

ASN



You may want to bookmark this pag

Stay on Track

Follow the path of your flight on your mobile device.

Have Fun!

©2010 Aircell. All rights reserved. G

Welcome to Gogo® on American Airlines!
Choose a pass to get started.

The page you attempted to view cannot be accessed until you purchase service.

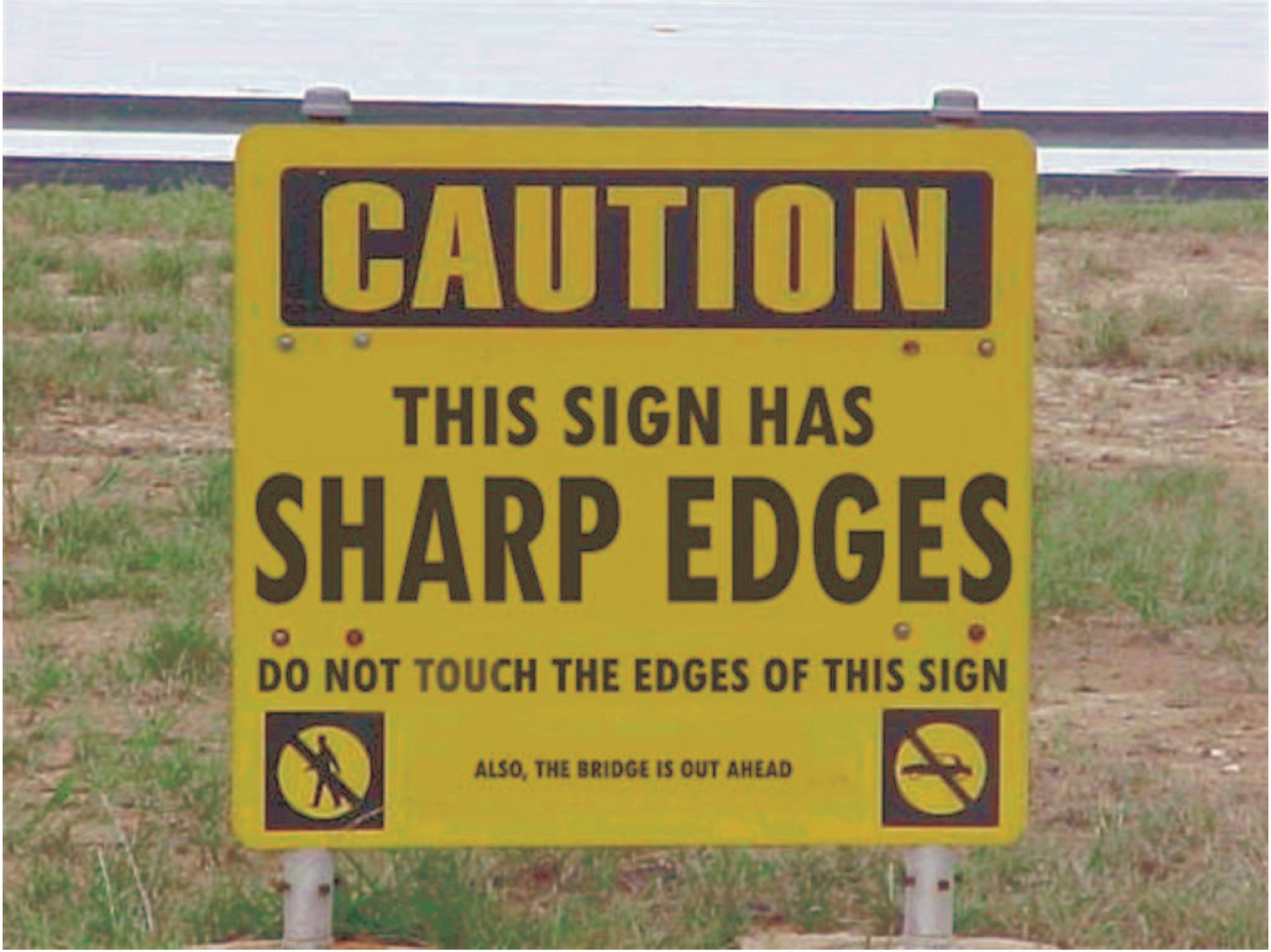
Gogo Mobile Flight Pass
$7.95
Connect using your mobile device during this flight.

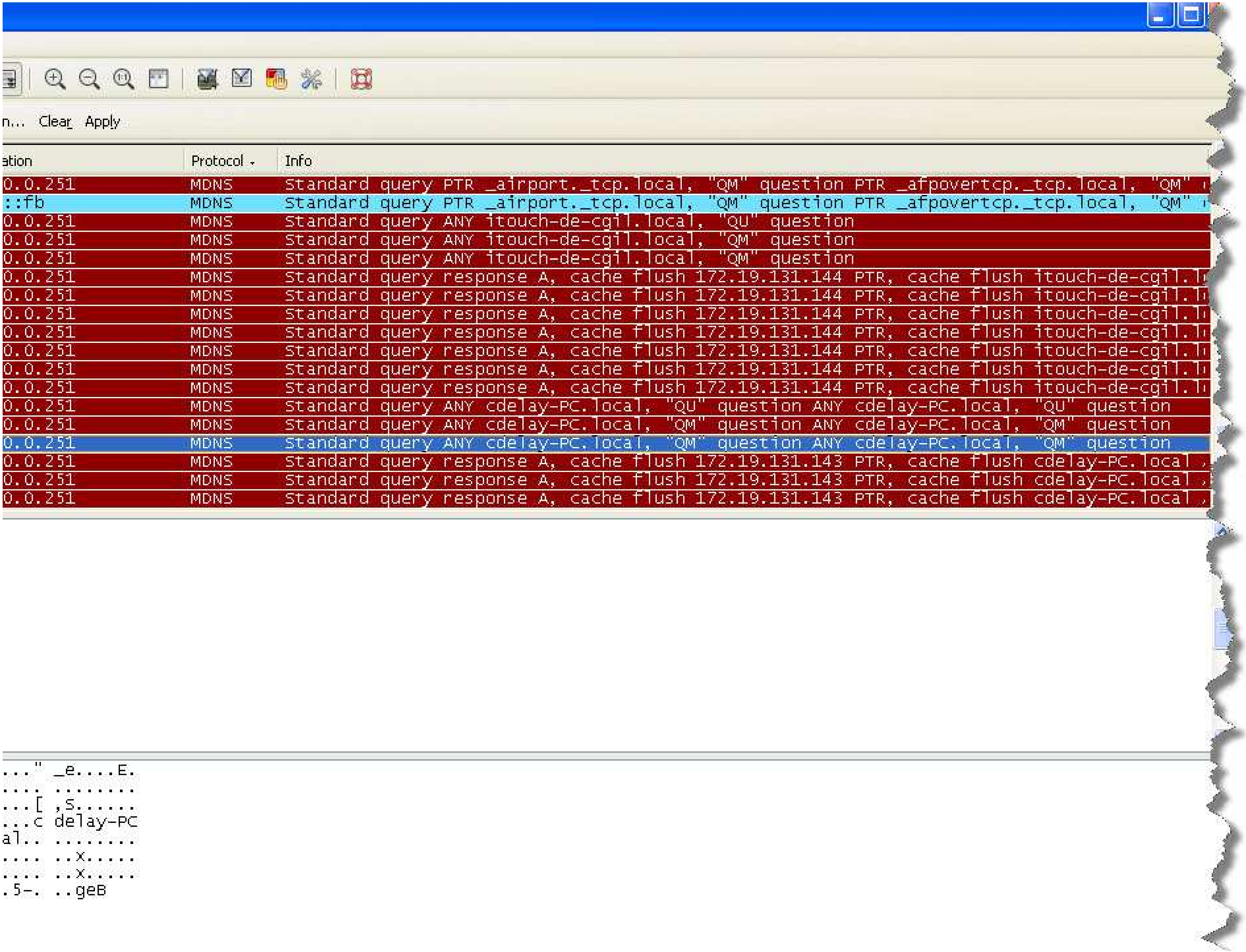
Gogo 30 Day Pass
$29.95

Have an active session?

Trust
mation Secu

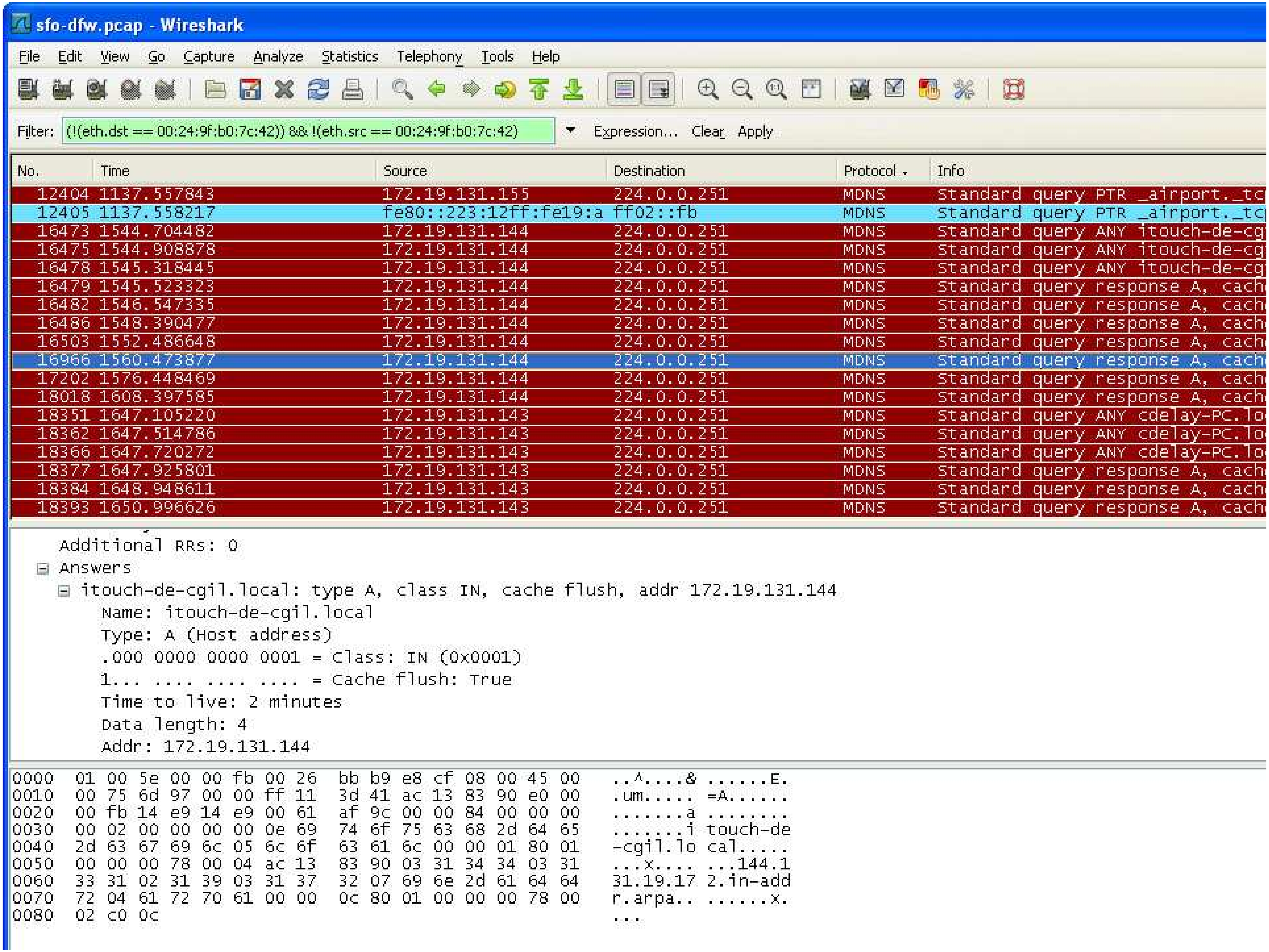
IS UMA SECURE?


CAUTION
THIS SIGN HAS
SHARP EDGES
DO NOT TOUCH THE EDGES OF THIS SIGN
ALSO, THE BRIDGE IS OUT AHEAD



```
ation                Protocol    Info
0.0.251              MDNS        Standard query PTR _airport._tcp.local, "QM" question PTR _afpovertcp._tcp.local, "QM"
::fb                 MDNS        Standard query PTR _airport._tcp.local, "QM" question PTR _afpovertcp._tcp.local, "QM"
0.0.251              MDNS        Standard query ANY itouch-de-cgil.local, "QU" question
0.0.251              MDNS        Standard query ANY itouch-de-cgil.local, "QM" question
0.0.251              MDNS        Standard query ANY itouch-de-cgil.local, "QM" question
0.0.251              MDNS        Standard query response A, cache flush 172.19.131.144 PTR, cache flush itouch-de-cgil.l
0.0.251              MDNS        Standard query response A, cache flush 172.19.131.144 PTR, cache flush itouch-de-cgil.l
0.0.251              MDNS        Standard query response A, cache flush 172.19.131.144 PTR, cache flush itouch-de-cgil.l
0.0.251              MDNS        Standard query response A, cache flush 172.19.131.144 PTR, cache flush itouch-de-cgil.l
0.0.251              MDNS        Standard query response A, cache flush 172.19.131.144 PTR, cache flush itouch-de-cgil.l
0.0.251              MDNS        Standard query response A, cache flush 172.19.131.144 PTR, cache flush itouch-de-cgil.l
0.0.251              MDNS        Standard query response A, cache flush 172.19.131.144 PTR, cache flush itouch-de-cgil.l
0.0.251              MDNS        Standard query ANY cdelay-PC.local, "QU" question ANY cdelay-PC.local, "QU" question
0.0.251              MDNS        Standard query ANY cdelay-PC.local, "QM" question ANY cdelay-PC.local, "QM" question
0.0.251              MDNS        Standard query ANY cdelay-PC.local, "QM" question ANY cdelay-PC.local, "QM" question
0.0.251              MDNS        Standard query response A, cache flush 172.19.131.143 PTR, cache flush cdelay-PC.local ,
0.0.251              MDNS        Standard query response A, cache flush 172.19.131.143 PTR, cache flush cdelay-PC.local ,
0.0.251              MDNS        Standard query response A, cache flush 172.19.131.143 PTR, cache flush cdelay-PC.local ,
```

```
..." _e....E.
.... ........
...[ ,S......
...c delay-PC
al.. ........
.... ..x.....
.... ..x.....
.5-. ..geB
```

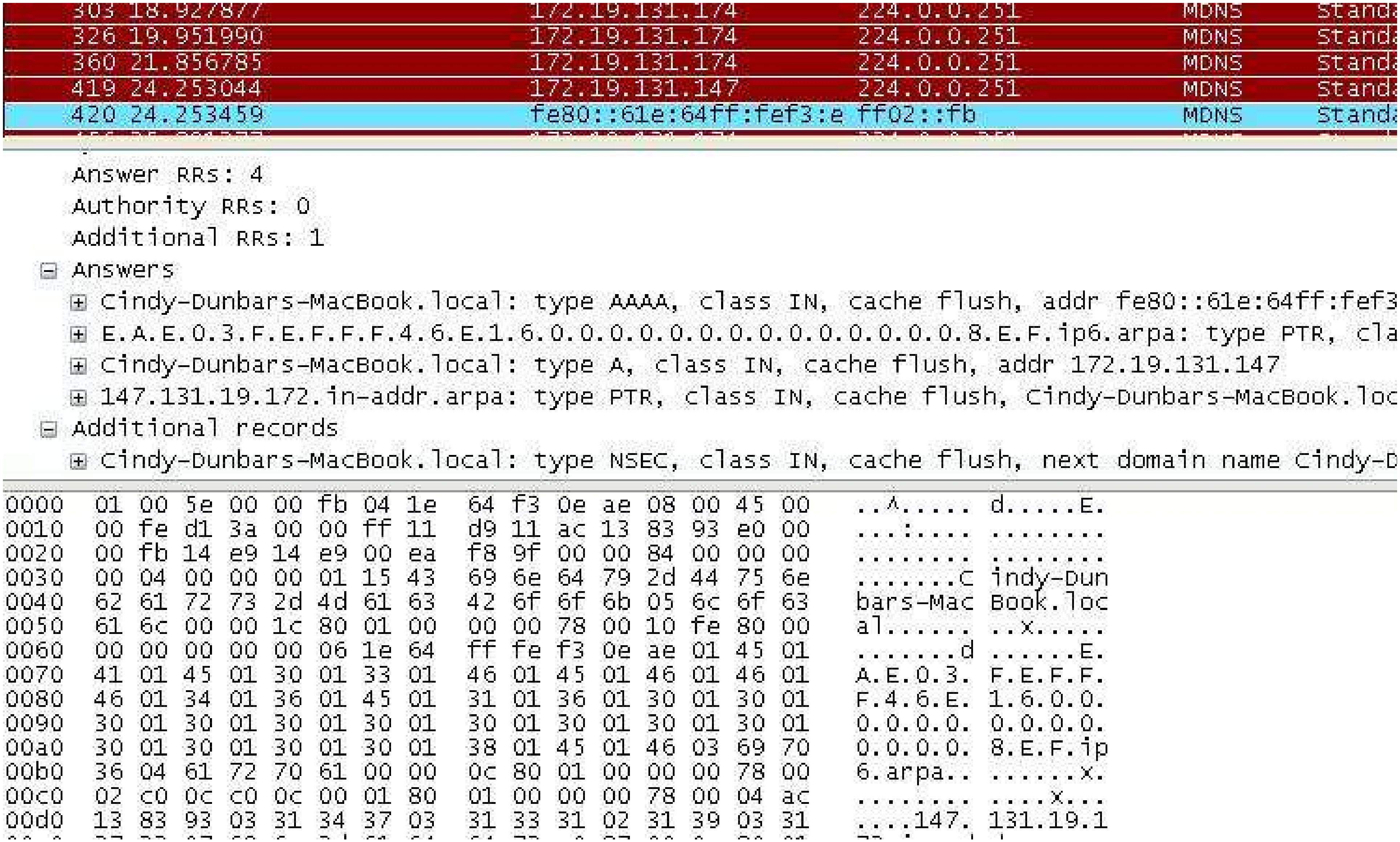

sfo-dfw.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

Filter: (!(eth.dst == 00:24:9f:b0:7c:42)) && !(eth.src == 00:24:9f:b0:7c:42)

```
No.   Time          Source                 Destination   Protocol  Info
12404 1137.557843   172.19.131.155         224.0.0.251   MDNS      Standard query PTR _airport._tc
12405 1137.558217   fe80::223:12ff:fe19:a  ff02::fb      MDNS      Standard query PTR _airport._tc
16473 1544.704482   172.19.131.144         224.0.0.251   MDNS      Standard query ANY itouch-de-cg
16475 1544.908878   172.19.131.144         224.0.0.251   MDNS      Standard query ANY itouch-de-cg
16478 1545.318445   172.19.131.144         224.0.0.251   MDNS      Standard query ANY itouch-de-cg
16479 1545.523323   172.19.131.144         224.0.0.251   MDNS      Standard query response A, cach
16482 1546.547335   172.19.131.144         224.0.0.251   MDNS      Standard query response A, cach
16486 1548.390477   172.19.131.144         224.0.0.251   MDNS      Standard query response A, cach
16503 1552.486648   172.19.131.144         224.0.0.251   MDNS      Standard query response A, cach
16966 1560.473877   172.19.131.144         224.0.0.251   MDNS      Standard query response A, cach
17202 1576.448469   172.19.131.144         224.0.0.251   MDNS      Standard query response A, cach
18018 1608.397585   172.19.131.144         224.0.0.251   MDNS      Standard query response A, cach
18351 1647.105220   172.19.131.143         224.0.0.251   MDNS      Standard query ANY cdelay-PC.lo
18362 1647.514786   172.19.131.143         224.0.0.251   MDNS      Standard query ANY cdelay-PC.lo
18366 1647.720272   172.19.131.143         224.0.0.251   MDNS      Standard query ANY cdelay-PC.lo
18377 1647.925801   172.19.131.143         224.0.0.251   MDNS      Standard query response A, cach
18384 1648.948611   172.19.131.143         224.0.0.251   MDNS      Standard query response A, cach
18393 1650.996626   172.19.131.143         224.0.0.251   MDNS      Standard query response A, cach
```

```
    Additional RRs: 0
  ⊟ Answers
    ⊟ itouch-de-cgil.local: type A, class IN, cache flush, addr 172.19.131.144
        Name: itouch-de-cgil.local
        Type: A (Host address)
        .000 0000 0000 0001 = Class: IN (0x0001)
        1... .... .... .... = Cache flush: True
        Time to live: 2 minutes
        Data length: 4
        Addr: 172.19.131.144
```

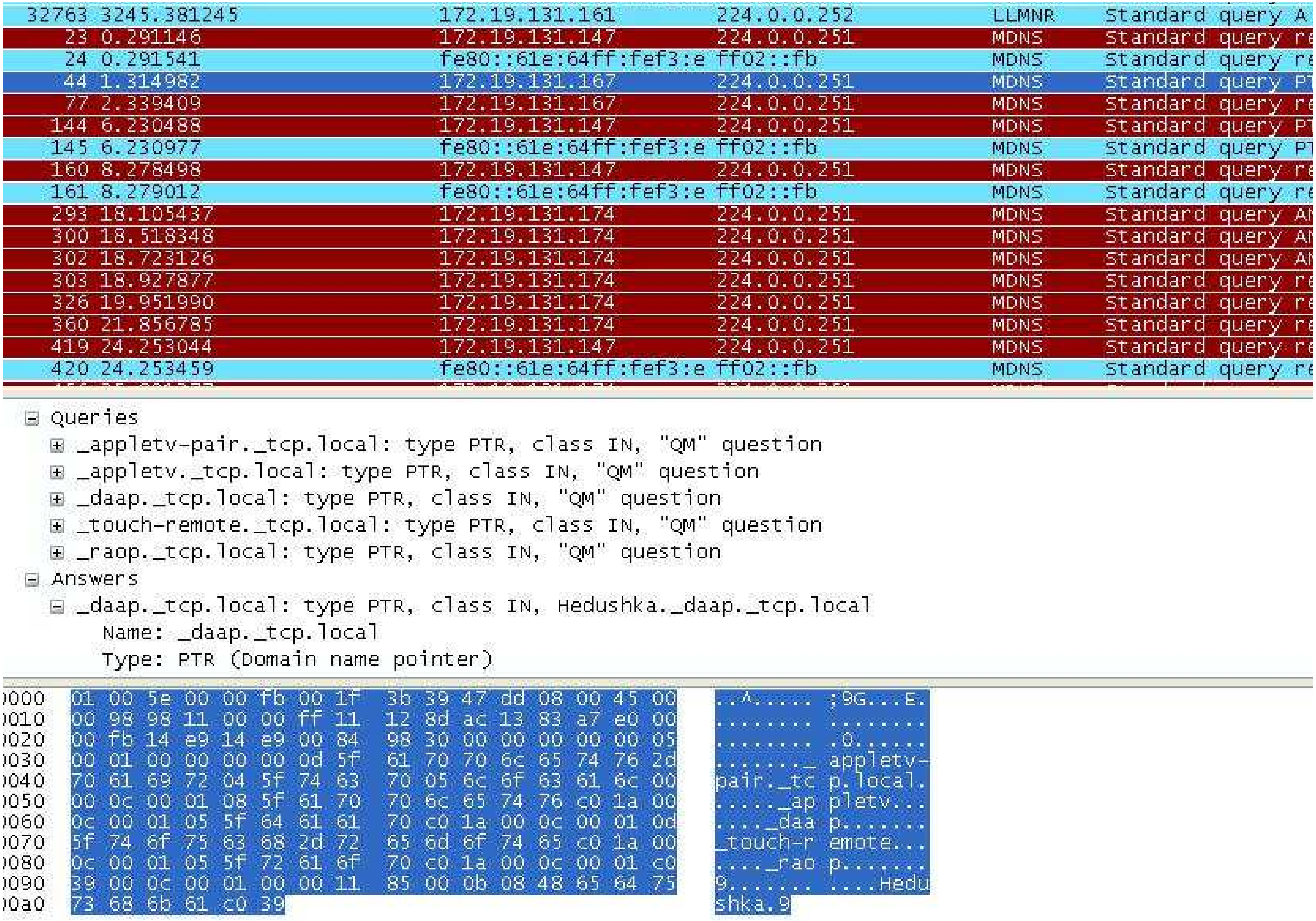
```
0000  01 00 5e 00 00 fb 00 26  bb b9 e8 cf 08 00 45 00   ..^....& ......E.
0010  00 75 6d 97 00 00 ff 11  3d 41 ac 13 83 90 e0 00   .um..... =A......
0020  00 fb 14 e9 14 e9 00 61  af 9c 00 00 84 00 00 00   .......a ........
0030  00 02 00 00 00 00 0e 69  74 6f 75 63 68 2d 64 65   .......i touch-de
0040  2d 63 67 69 6c 05 6c 6f  63 61 6c 00 00 01 80 01   -cgil.lo cal.....
0050  00 00 00 78 00 04 ac 13  83 90 03 31 34 34 03 31   ...x.... ...144.1
0060  33 31 02 31 39 03 31 37  32 07 69 6e 2d 61 64 64   31.19.17 2.in-add
0070  72 04 61 72 70 61 00 00  0c 80 01 00 00 00 78 00   r.arpa.. ......x.
0080  02 c0 0c                                           ...
```



```
 303 18.927877      172.19.131.174     224.0.0.251      MDNS    Standa
 326 19.951990      172.19.131.174     224.0.0.251      MDNS    Standa
 360 21.856785      172.19.131.174     224.0.0.251      MDNS    Standa
 419 24.253044      172.19.131.147     224.0.0.251      MDNS    Standa
 420 24.253459      fe80::61e:64ff:fef3:e ff02::fb      MDNS    Standa
```

```
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 1
  ⊟ Answers
    ⊞ Cindy-Dunbars-MacBook.local: type AAAA, class IN, cache flush, addr fe80::61e:64ff:fef3
    ⊞ E.A.E.0.3.F.E.F.F.F.4.6.E.1.6.0.0.0.0.0.0.0.0.0.0.0.0.0.8.E.F.ip6.arpa: type PTR, cla
    ⊞ Cindy-Dunbars-MacBook.local: type A, class IN, cache flush, addr 172.19.131.147
    ⊞ 147.131.19.172.in-addr.arpa: type PTR, class IN, cache flush, Cindy-Dunbars-MacBook.loc
  ⊟ Additional records
    ⊞ Cindy-Dunbars-MacBook.local: type NSEC, class IN, cache flush, next domain name Cindy-D
```

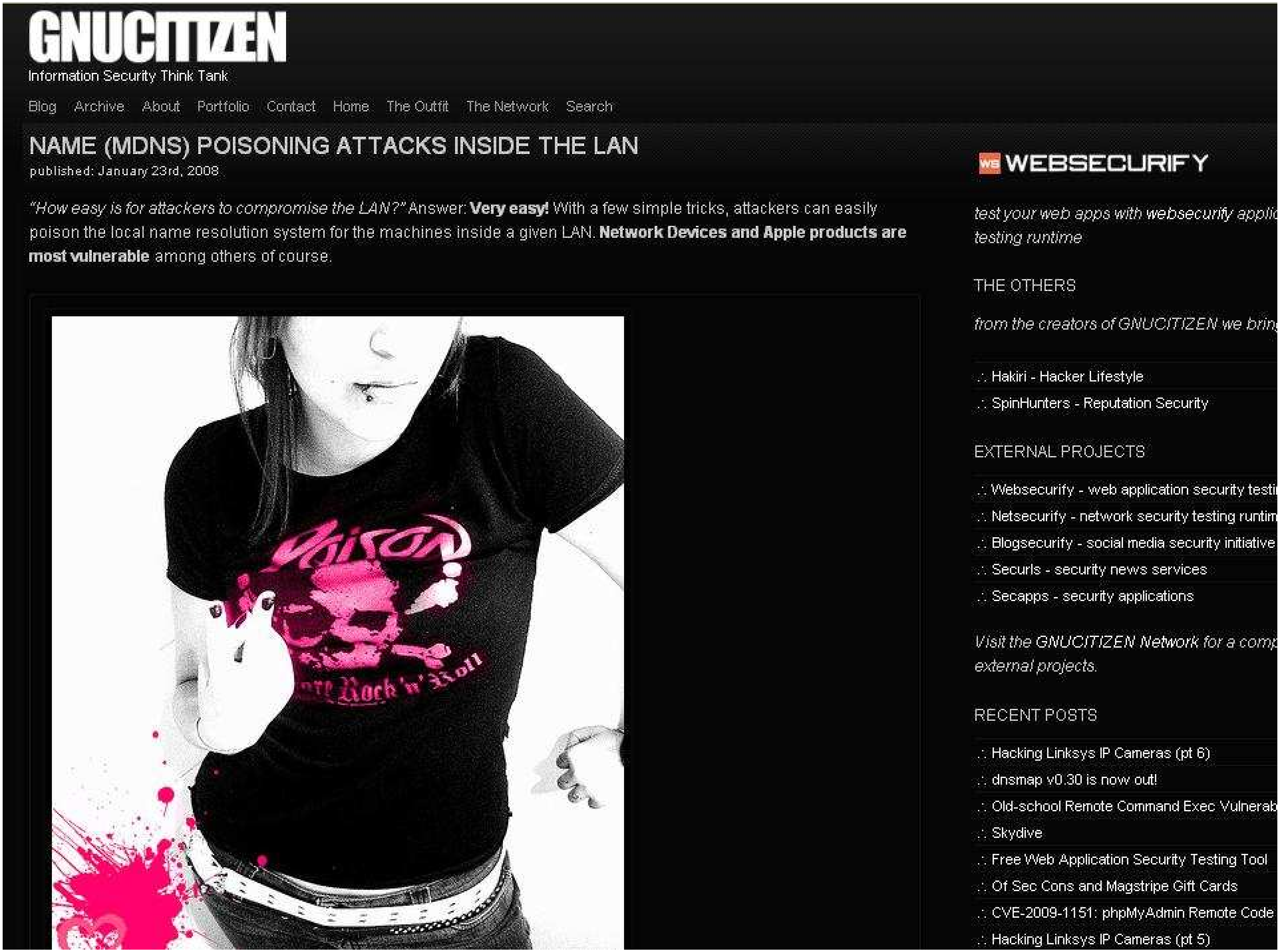
```
0000  01 00 5e 00 00 fb 04 1e  64 f3 0e ae 08 00 45 00   ..^..... d.....E.
0010  00 fe d1 3a 00 00 ff 11  d9 11 ac 13 83 93 e0 00   ...:.... ........
0020  00 fb 14 e9 14 e9 00 ea  f8 9f 00 00 84 00 00 00   ........ ........
0030  00 04 00 00 00 01 15 43  69 6e 64 79 2d 44 75 6e   .......C indy-Dun
0040  62 61 72 73 2d 4d 61 63  42 6f 6f 6b 05 6c 6f 63   bars-Mac Book.loc
0050  61 6c 00 00 1c 80 01 00  00 00 78 00 10 fe 80 00   al...... ..x.....
0060  00 00 00 00 00 06 1e 64  ff fe f3 0e ae 01 45 01   .......d ......E.
0070  41 01 45 01 30 01 33 01  46 01 45 01 46 01 46 01   A.E.0.3. F.E.F.F.
0080  46 01 34 01 36 01 45 01  31 01 36 01 30 01 30 01   F.4.6.E. 1.6.0.0.
0090  30 01 30 01 30 01 30 01  30 01 30 01 30 01 30 01   0.0.0.0. 0.0.0.0.
00a0  30 01 30 01 30 01 30 01  38 01 45 01 46 03 69 70   0.0.0.0. 8.E.F.ip
00b0  36 04 61 72 70 61 00 00  0c 80 01 00 00 00 78 00   6.arpa.. ......x.
00c0  02 c0 0c c0 0c 00 01 80  01 00 00 00 78 00 04 ac   ........ ....x...
00d0  13 83 93 03 31 34 37 03  31 33 31 02 31 39 03 31   ....147. 131.19.1
```



```
32763 3245.381245   172.19.131.161          224.0.0.252   LLMNR   Standard query A
   23 0.291146      172.19.131.147          224.0.0.251   MDNS    Standard query re
   24 0.291541      fe80::61e:64ff:fef3:e ff02::fb        MDNS    Standard query re
   44 1.314982      172.19.131.167          224.0.0.251   MDNS    Standard query PT
   77 2.339409      172.19.131.167          224.0.0.251   MDNS    Standard query re
  144 6.230488      172.19.131.147          224.0.0.251   MDNS    Standard query PT
  145 6.230977      fe80::61e:64ff:fef3:e ff02::fb        MDNS    Standard query PT
  160 8.278498      172.19.131.147          224.0.0.251   MDNS    Standard query re
  161 8.279012      fe80::61e:64ff:fef3:e ff02::fb        MDNS    Standard query re
  293 18.105437     172.19.131.174          224.0.0.251   MDNS    Standard query AN
  300 18.518348     172.19.131.174          224.0.0.251   MDNS    Standard query AN
  302 18.723126     172.19.131.174          224.0.0.251   MDNS    Standard query AN
  303 18.927877     172.19.131.174          224.0.0.251   MDNS    Standard query re
  326 19.951990     172.19.131.174          224.0.0.251   MDNS    Standard query re
  360 21.856785     172.19.131.174          224.0.0.251   MDNS    Standard query re
  419 24.253044     172.19.131.147          224.0.0.251   MDNS    Standard query re
  420 24.253459     fe80::61e:64ff:fef3:e ff02::fb        MDNS    Standard query re
```

```
⊟ Queries
   ⊞ _appletv-pair._tcp.local: type PTR, class IN, "QM" question
   ⊞ _appletv._tcp.local: type PTR, class IN, "QM" question
   ⊞ _daap._tcp.local: type PTR, class IN, "QM" question
   ⊞ _touch-remote._tcp.local: type PTR, class IN, "QM" question
   ⊞ _raop._tcp.local: type PTR, class IN, "QM" question
⊟ Answers
   ⊟ _daap._tcp.local: type PTR, class IN, Hedushka._daap._tcp.local
       Name: _daap._tcp.local
       Type: PTR (Domain name pointer)
```

```
0000   01 00 5e 00 00 fb 00 1f  3b 39 47 dd 08 00 45 00   ..^..... ;9G...E.
0010   00 98 98 11 00 00 ff 11  12 8d ac 13 83 a7 e0 00   ........ ........
0020   00 fb 14 e9 14 e9 00 84  98 30 00 00 00 00 00 05   ........ .0......
0030   00 01 00 00 00 00 0d 5f  61 70 70 6c 65 74 76 2d   ......._ appletv-
0040   70 61 69 72 04 5f 74 63  70 05 6c 6f 63 61 6c 00   pair._tc p.local.
0050   00 0c 00 01 08 5f 61 70  70 6c 65 74 76 c0 1a 00   ....._ap pletv...
0060   0c 00 01 05 5f 64 61 61  70 c0 1a 00 0c 00 01 0d   ...._daa p.......
0070   5f 74 6f 75 63 68 2d 72  65 6d 6f 74 65 c0 1a 00   _touch-r emote...
0080   0c 00 01 05 5f 72 61 6f  70 c0 1a 00 0c 00 01 c0   ...._rao p.......
0090   39 00 0c 00 01 00 00 11  85 00 0b 08 48 65 64 75   9....... ....Hedu
00a0   73 68 6b 61 c0 39                                  shka.9
```



GNUCITIZEN

Information Security Think Tank

Blog Archive About Portfolio Contact Home The Outfit The Network Search

NAME (MDNS) POISONING ATTACKS INSIDE THE LAN

published: January 23rd, 2008

"How easy is for attackers to compromise the LAN?" Answer: **Very easy!** With a few simple tricks, attackers can easily poison the local name resolution system for the machines inside a given LAN. **Network Devices and Apple products are most vulnerable** among others of course.

test your web apps with websecurify applic
testing runtime

THE OTHERS

from the creators of GNUCITIZEN we brin

.: Hakiri - Hacker Lifestyle
.: SpinHunters - Reputation Security

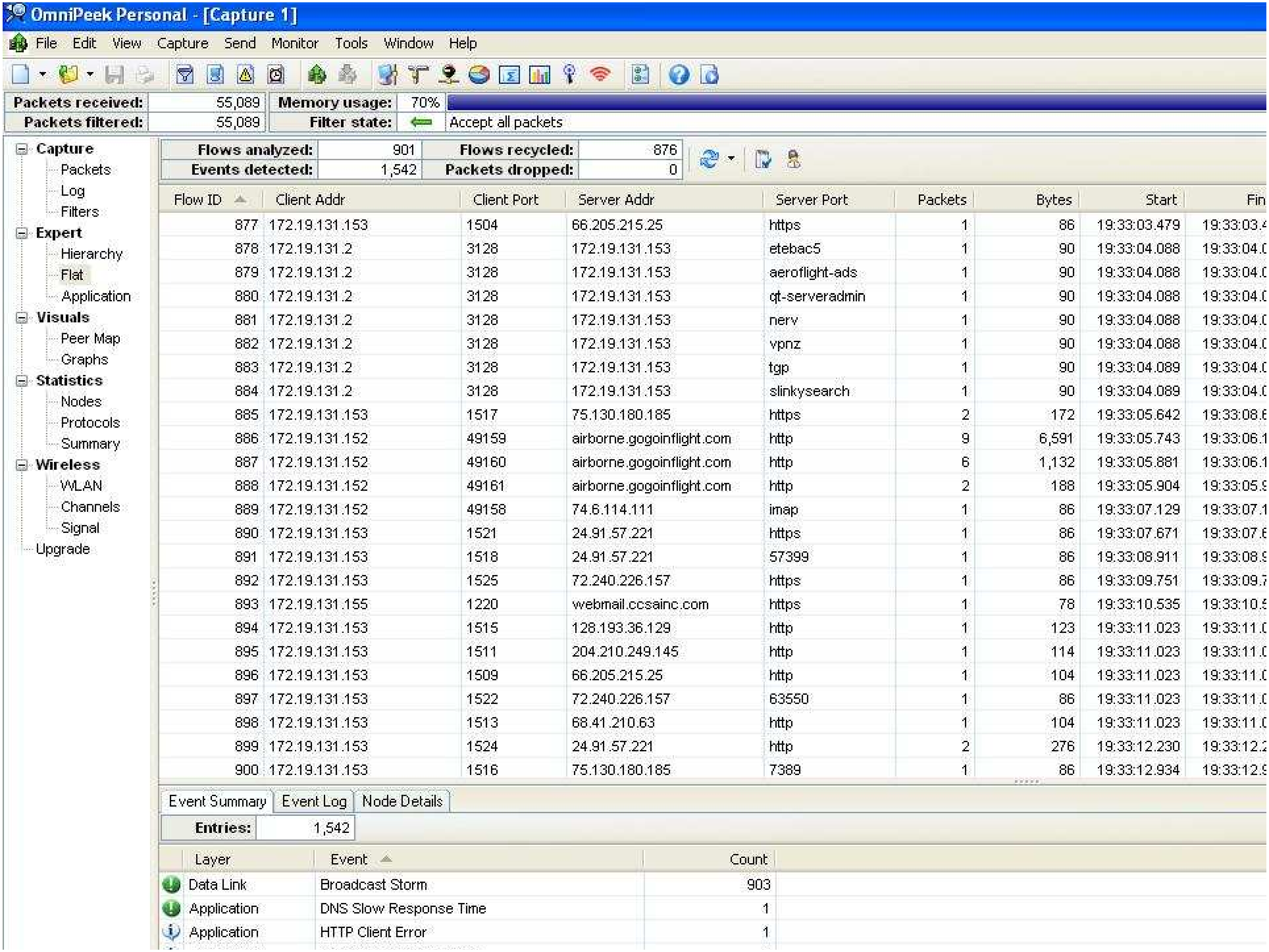
EXTERNAL PROJECTS

.: Websecurify - web application security testi
.: Netsecurify - network security testing runtim
.: Blogsecurify - social media security initiative
.: Securls - security news services
.: Secapps - security applications

Visit the GNUCITIZEN Network for a comp
external projects.

RECENT POSTS

.: Hacking Linksys IP Cameras (pt 6)
.: dnsmap v0.30 is now out!
.: Old-school Remote Command Exec Vulnerab
.: Skydive
.: Free Web Application Security Testing Tool
.: Of Sec Cons and Magstripe Gift Cards
.: CVE-2009-1151: phpMyAdmin Remote Code
.: Hacking Linksys IP Cameras (pt 5)



OmniPeek Personal - [Capture 1]
File Edit View Capture Send Monitor Tools Window Help

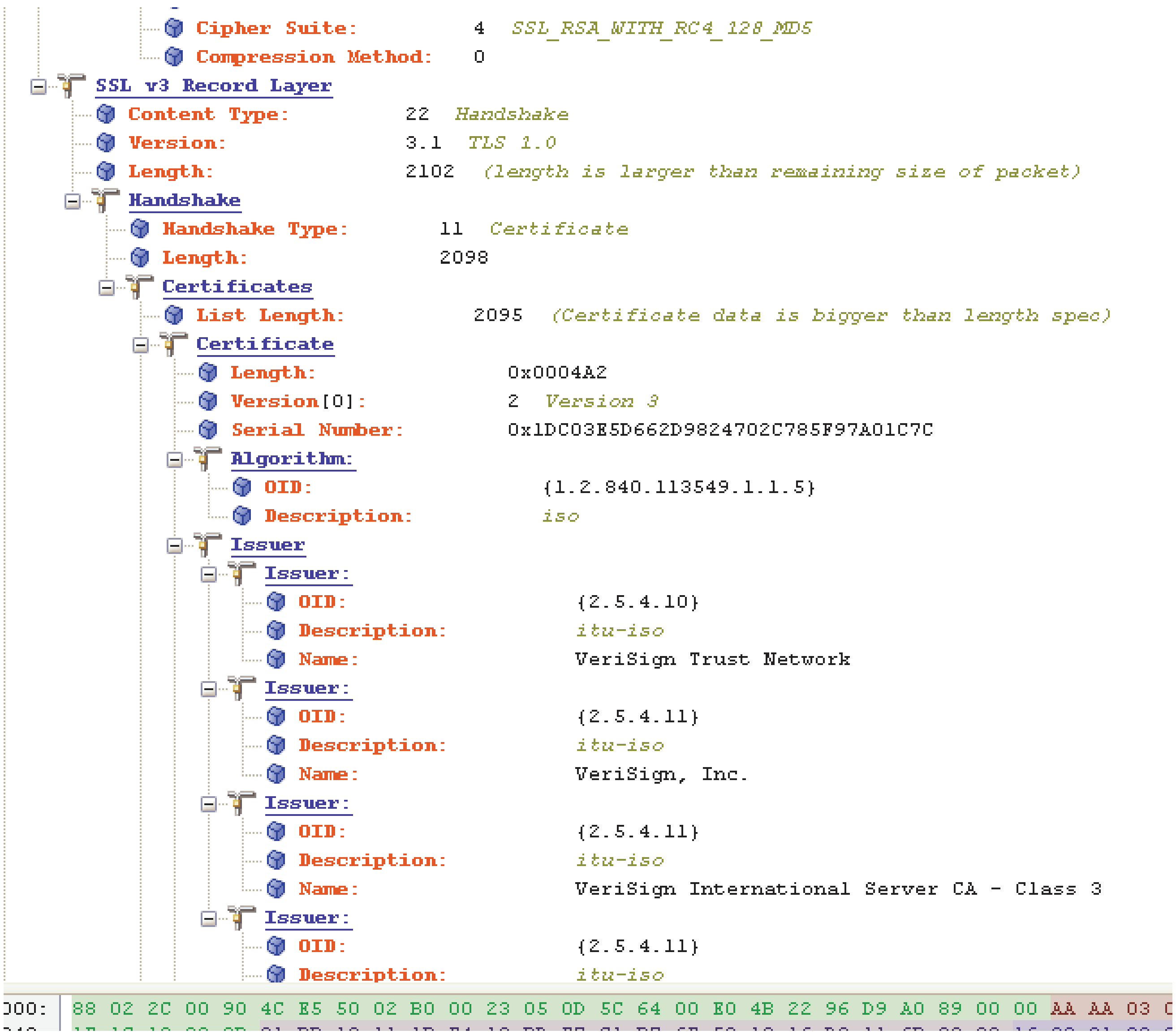
Packets received:	55,089	Memory usage:	70%	
Packets filtered:	55,089	Filter state:		Accept all packets

Flows analyzed:	901	Flows recycled:	876
Events detected:	1,542	Packets dropped:	0

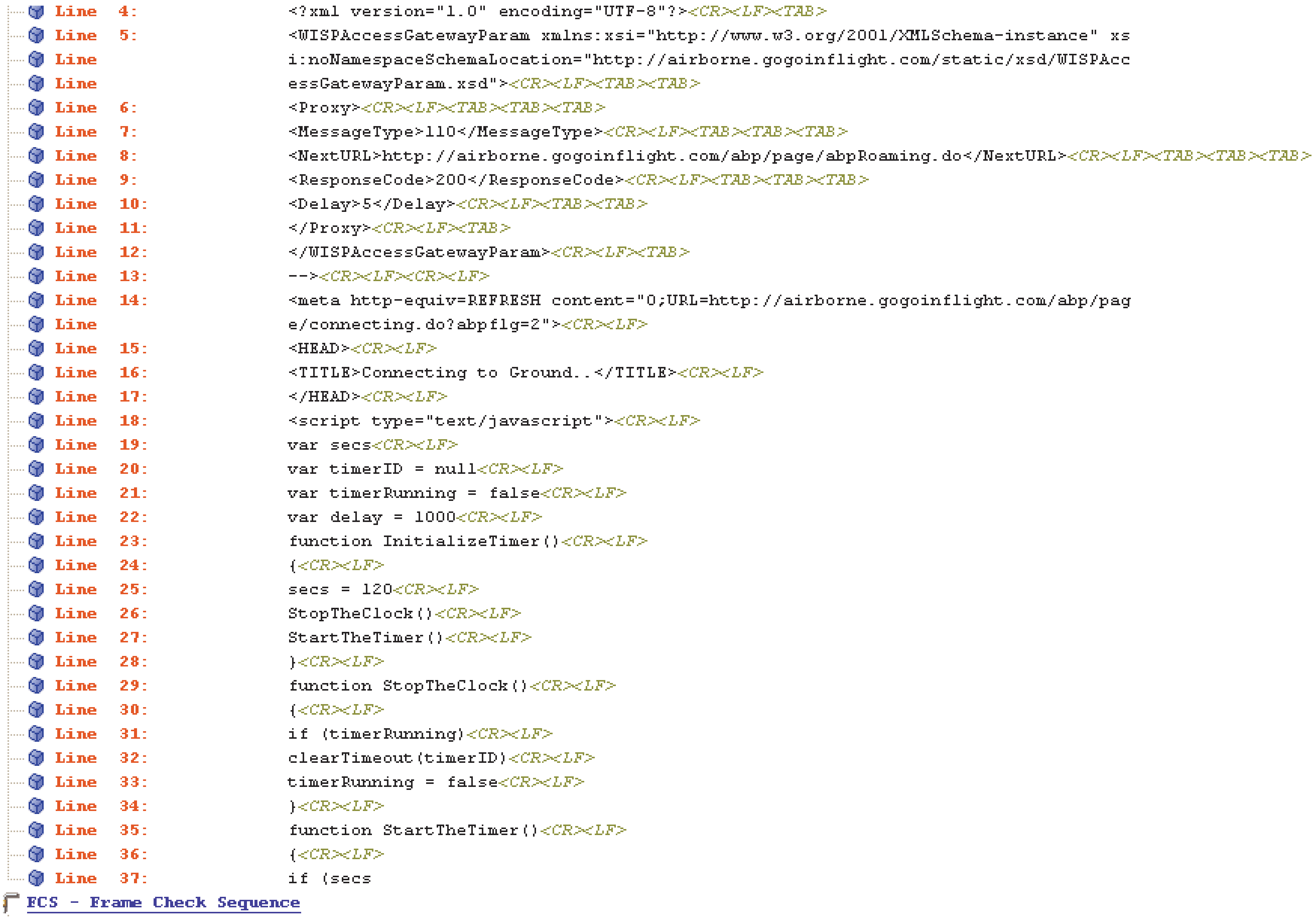
Flow ID	Client Addr	Client Port	Server Addr	Server Port	Packets	Bytes	Start	Fin
877	172.19.131.153	1504	66.205.215.25	https	1	86	19:33:03.479	19:33:03.4
878	172.19.131.2	3128	172.19.131.153	etebac5	1	90	19:33:04.088	19:33:04.0
879	172.19.131.2	3128	172.19.131.153	aeroflight-ads	1	90	19:33:04.088	19:33:04.0
880	172.19.131.2	3128	172.19.131.153	qt-serveradmin	1	90	19:33:04.088	19:33:04.0
881	172.19.131.2	3128	172.19.131.153	nerv	1	90	19:33:04.088	19:33:04.0
882	172.19.131.2	3128	172.19.131.153	vpnz	1	90	19:33:04.088	19:33:04.0
883	172.19.131.2	3128	172.19.131.153	tgp	1	90	19:33:04.089	19:33:04.0
884	172.19.131.2	3128	172.19.131.153	slinkysearch	1	90	19:33:04.089	19:33:04.0
885	172.19.131.153	1517	75.130.180.185	https	2	172	19:33:05.642	19:33:08.6
886	172.19.131.152	49159	airborne.gogoinflight.com	http	9	6,591	19:33:05.743	19:33:06.1
887	172.19.131.152	49160	airborne.gogoinflight.com	http	6	1,132	19:33:05.881	19:33:06.1
888	172.19.131.152	49161	airborne.gogoinflight.com	http	2	188	19:33:05.904	19:33:05.9
889	172.19.131.152	49158	74.6.114.111	imap	1	86	19:33:07.129	19:33:07.1
890	172.19.131.153	1521	24.91.57.221	https	1	86	19:33:07.671	19:33:07.6
891	172.19.131.153	1518	24.91.57.221	57399	1	86	19:33:08.911	19:33:08.9
892	172.19.131.153	1525	72.240.226.157	https	1	86	19:33:09.751	19:33:09.7
893	172.19.131.155	1220	webmail.ccsainc.com	https	1	78	19:33:10.535	19:33:10.5
894	172.19.131.153	1515	128.193.36.129	http	1	123	19:33:11.023	19:33:11.0
895	172.19.131.153	1511	204.210.249.145	http	1	114	19:33:11.023	19:33:11.0
896	172.19.131.153	1509	66.205.215.25	http	1	104	19:33:11.023	19:33:11.0
897	172.19.131.153	1522	72.240.226.157	63550	1	86	19:33:11.023	19:33:11.0
898	172.19.131.153	1513	68.41.210.63	http	1	104	19:33:11.023	19:33:11.0
899	172.19.131.153	1524	24.91.57.221	http	2	276	19:33:12.230	19:33:12.2
900	172.19.131.153	1516	75.130.180.185	7389	1	86	19:33:12.934	19:33:12.9

Entries: 1,542

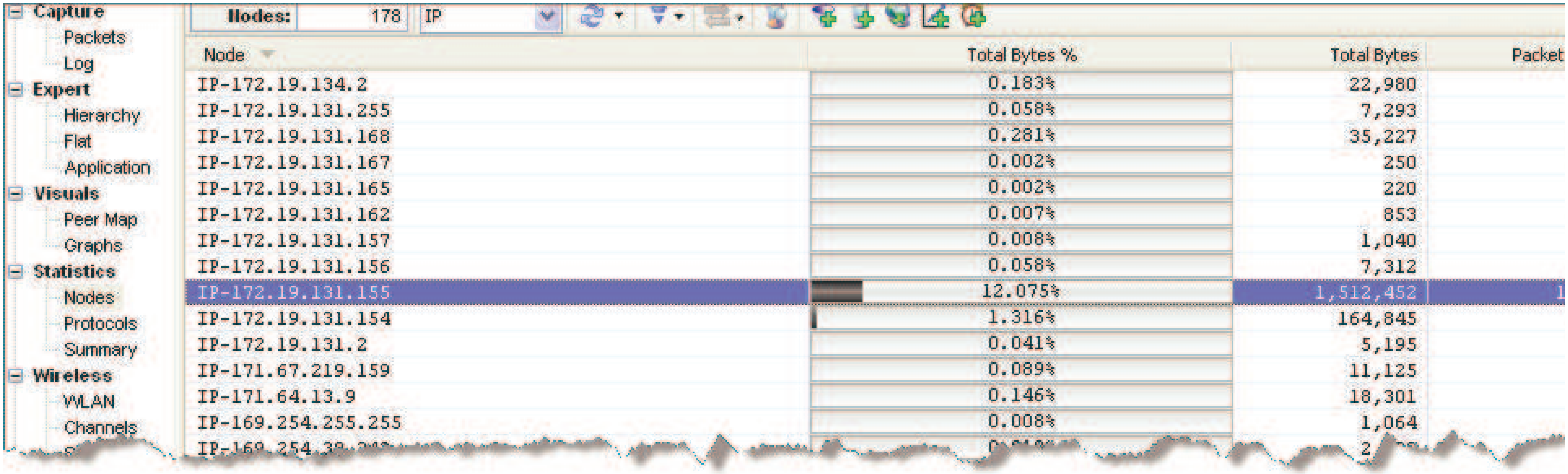
Layer	Event	Count
Data Link	Broadcast Storm	903
Application	DNS Slow Response Time	1
Application	HTTP Client Error	1



```
        Cipher Suite:           4   SSL_RSA_WITH_RC4_128_MD5
        Compression Method:     0
SSL v3 Record Layer
    Content Type:           22   Handshake
    Version:                3.1   TLS 1.0
    Length:                 2102   (length is larger than remaining size of packet)
    Handshake
        Handshake Type:         11   Certificate
        Length:                 2098
        Certificates
            List Length:            2095   (Certificate data is bigger than length spec)
            Certificate
                Length:                 0x0004A2
                Version[0]:             2   Version 3
                Serial Number:          0x1DC03E5D662D9824702C785F97A01C7C
                Algorithm:
                    OID:                    {1.2.840.113549.1.1.5}
                    Description:            iso
                Issuer
                    Issuer:
                        OID:                    {2.5.4.10}
                        Description:            itu-iso
                        Name:                   VeriSign Trust Network
                    Issuer:
                        OID:                    {2.5.4.11}
                        Description:            itu-iso
                        Name:                   VeriSign, Inc.
                    Issuer:
                        OID:                    {2.5.4.11}
                        Description:            itu-iso
                        Name:                   VeriSign International Server CA - Class 3
                    Issuer:
                        OID:                    {2.5.4.11}
                        Description:            itu-iso
)00: 88 02 2C 00 90 4C E5 50 02 B0 00 23 05 0D 5C 64 00 E0 4B 22 96 D9 A0 89 00 00 AA AA 03 C
```

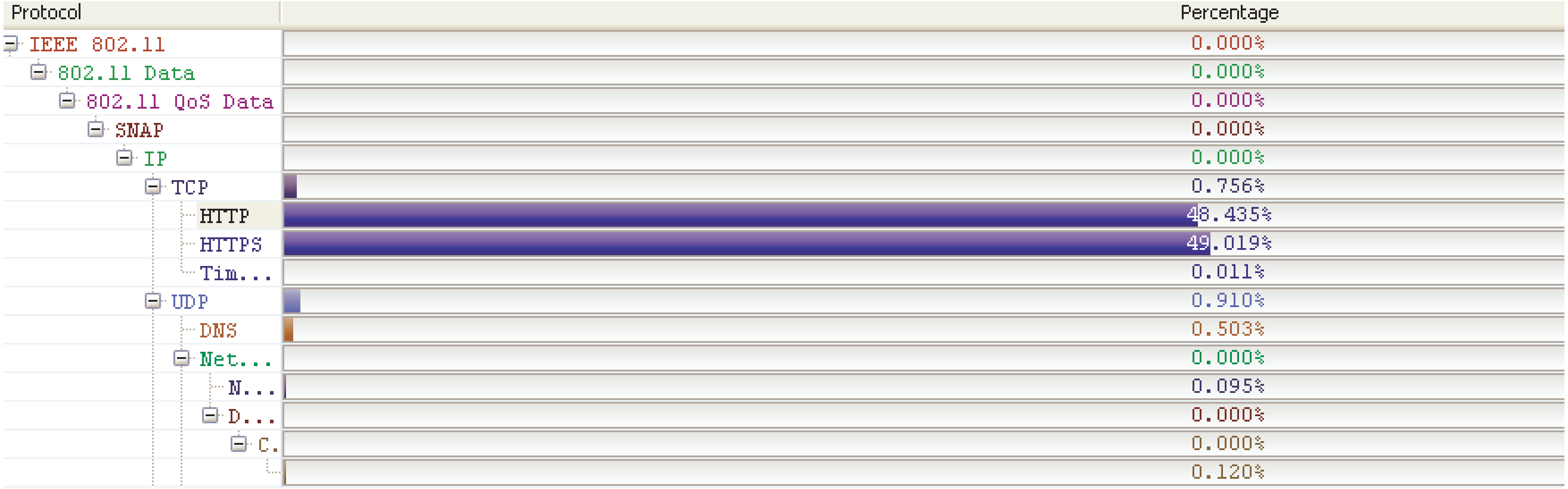


```
Line  4:        <?xml version="1.0" encoding="UTF-8"?><CR><LF><TAB>
Line  5:        <WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xs
Line            i:noNamespaceSchemaLocation="http://airborne.gogoinflight.com/static/xsd/WISPAcc
Line            essGatewayParam.xsd"><CR><LF><TAB><TAB>
Line  6:        <Proxy><CR><LF><TAB><TAB><TAB>
Line  7:        <MessageType>110</MessageType><CR><LF><TAB><TAB><TAB>
Line  8:        <NextURL>http://airborne.gogoinflight.com/abp/page/abpRoaming.do</NextURL><CR><LF><TAB><TAB><TAB>
Line  9:        <ResponseCode>200</ResponseCode><CR><LF><TAB><TAB><TAB>
Line 10:        <Delay>5</Delay><CR><LF><TAB><TAB>
Line 11:        </Proxy><CR><LF><TAB>
Line 12:        </WISPAccessGatewayParam><CR><LF><TAB>
Line 13:        --><CR><LF><CR><LF>
Line 14:        <meta http-equiv=REFRESH content="0;URL=http://airborne.gogoinflight.com/abp/pag
Line            e/connecting.do?abpflg=2"><CR><LF>
Line 15:        <HEAD><CR><LF>
Line 16:        <TITLE>Connecting to Ground..</TITLE><CR><LF>
Line 17:        </HEAD><CR><LF>
Line 18:        <script type="text/javascript"><CR><LF>
Line 19:        var secs<CR><LF>
Line 20:        var timerID = null<CR><LF>
Line 21:        var timerRunning = false<CR><LF>
Line 22:        var delay = 1000<CR><LF>
Line 23:        function InitializeTimer()<CR><LF>
Line 24:        {<CR><LF>
Line 25:        secs = 120<CR><LF>
Line 26:        StopTheClock()<CR><LF>
Line 27:        StartTheTimer()<CR><LF>
Line 28:        }<CR><LF>
Line 29:        function StopTheClock()<CR><LF>
Line 30:        {<CR><LF>
Line 31:        if (timerRunning)<CR><LF>
Line 32:        clearTimeout(timerID)<CR><LF>
Line 33:        timerRunning = false<CR><LF>
Line 34:        }<CR><LF>
Line 35:        function StartTheTimer()<CR><LF>
Line 36:        {<CR><LF>
Line 37:        if (secs
FCS - Frame Check Sequence
```

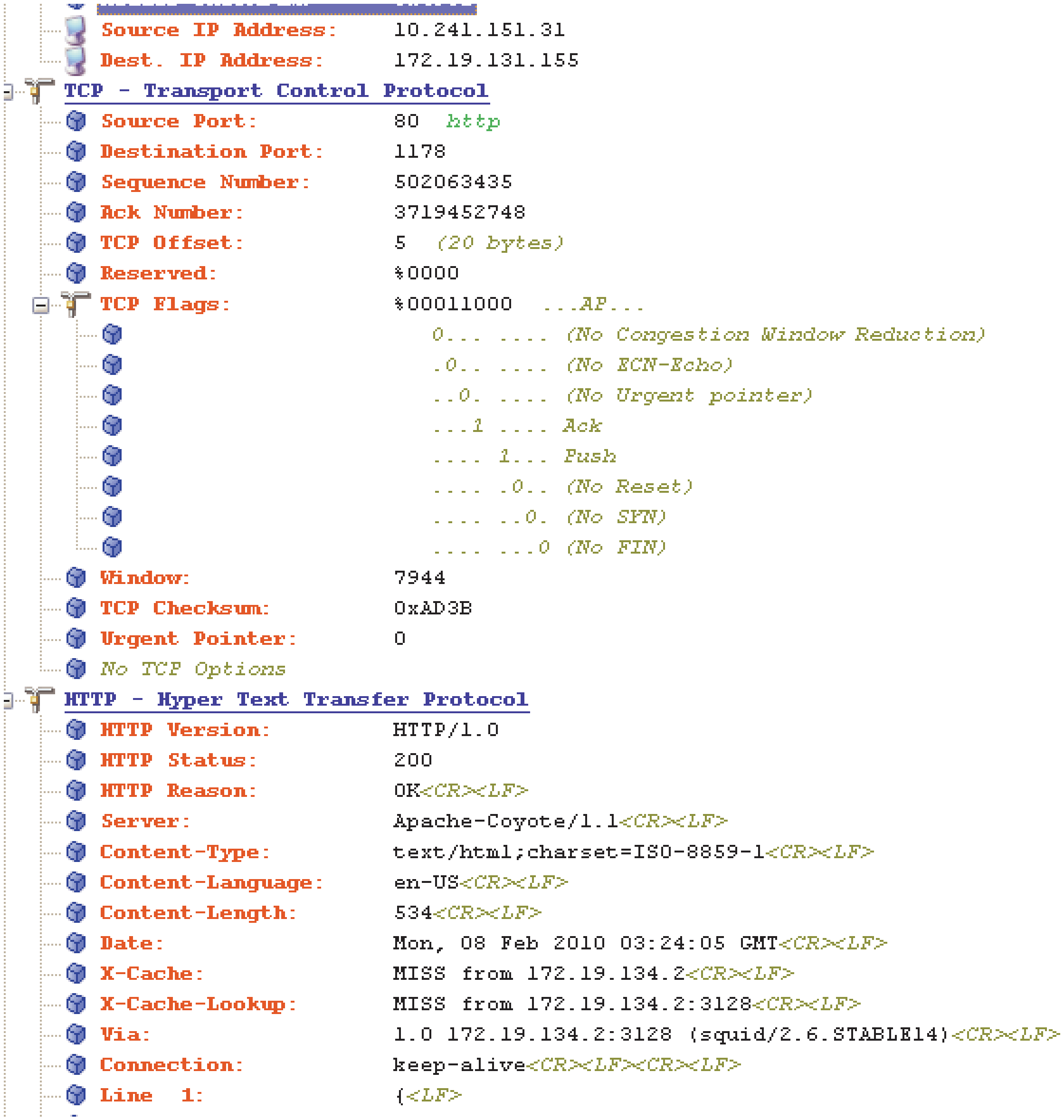


Nodes: 178 IP

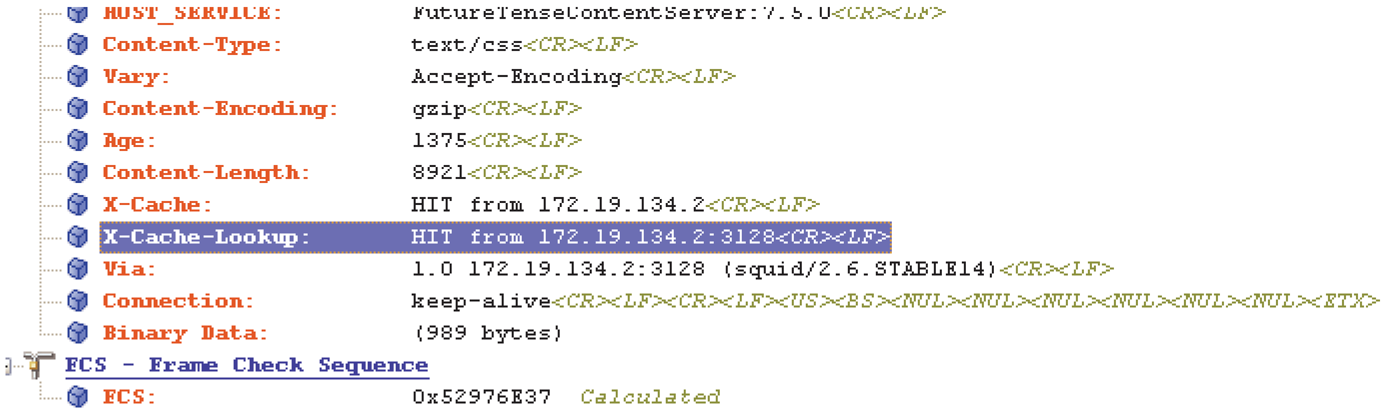
Node	Total Bytes %	Total Bytes	Packet
IP-172.19.134.2	0.183%	22,980	
IP-172.19.131.255	0.058%	7,293	
IP-172.19.131.168	0.281%	35,227	
IP-172.19.131.167	0.002%	250	
IP-172.19.131.165	0.002%	220	
IP-172.19.131.162	0.007%	853	
IP-172.19.131.157	0.008%	1,040	
IP-172.19.131.156	0.058%	7,312	
IP-172.19.131.155	12.075%	1,512,452	1
IP-172.19.131.154	1.316%	164,845	
IP-172.19.131.2	0.041%	5,195	
IP-171.67.219.159	0.089%	11,125	
IP-171.64.13.9	0.146%	18,301	
IP-169.254.255.255	0.008%	1,064	
IP-169.254.3[illegible]	0.01[illegible]	2[illegible]	



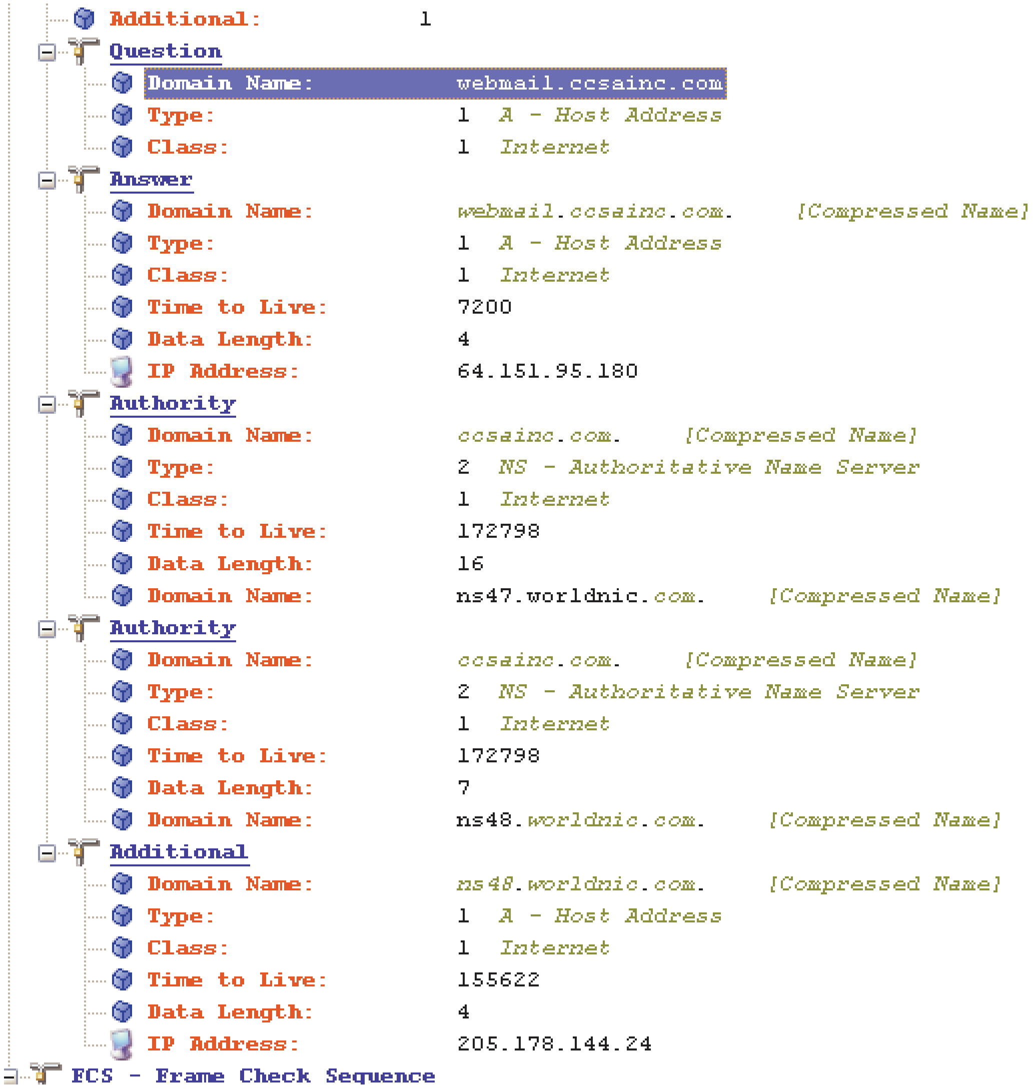
Protocol	Percentage
IEEE 802.11	0.000%
802.11 Data	0.000%
802.11 QoS Data	0.000%
SNAP	0.000%
IP	0.000%
TCP	0.756%
HTTP	48.435%
HTTPS	49.019%
Tim...	0.011%
UDP	0.910%
DNS	0.503%
Net...	0.000%
N...	0.095%
D...	0.000%
C.	0.000%
	0.120%



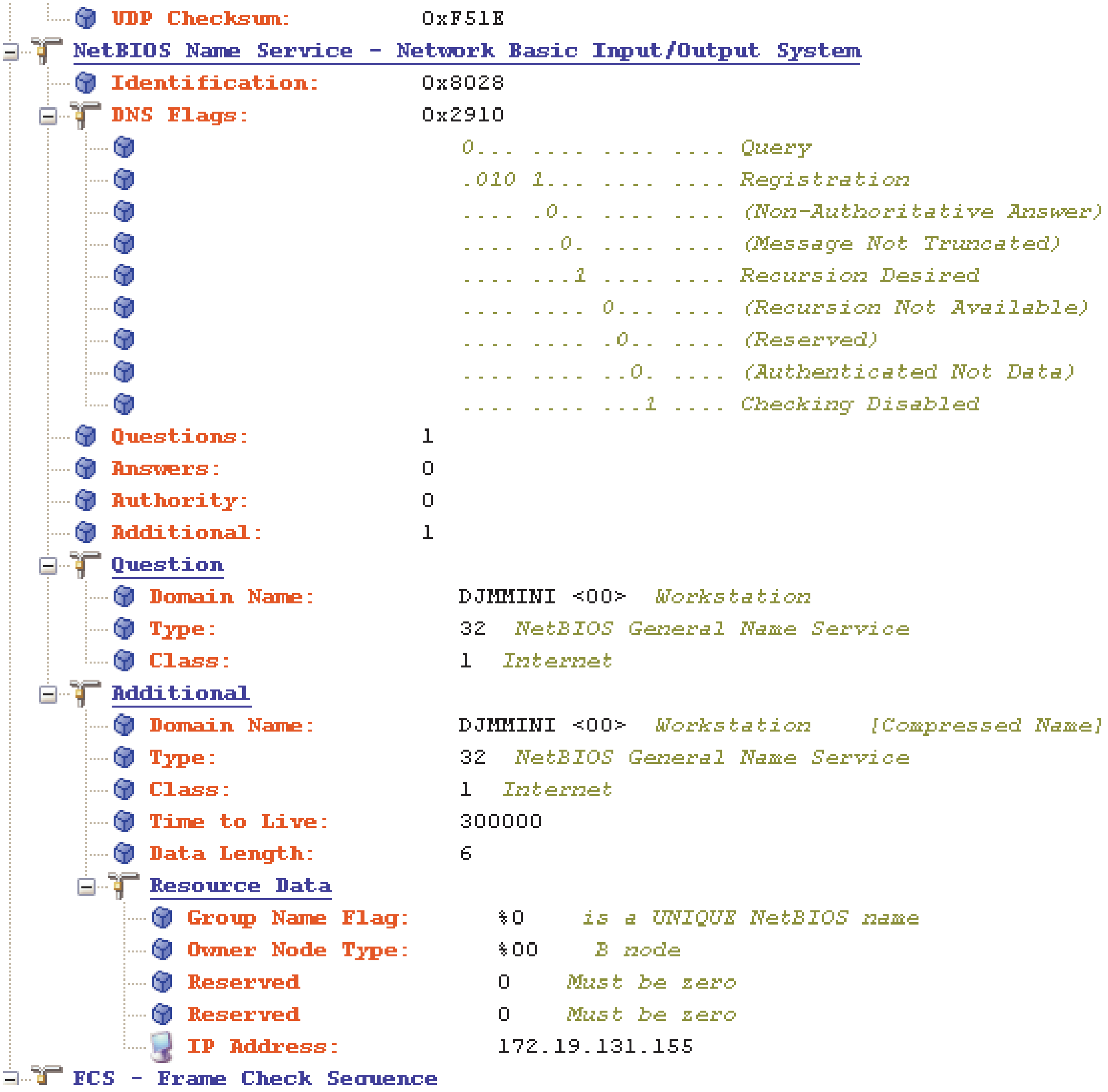
```
    Source IP Address:      10.241.151.31
    Dest. IP Address:       172.19.131.155
TCP - Transport Control Protocol
    Source Port:            80  http
    Destination Port:       1178
    Sequence Number:        502063435
    Ack Number:             3719452748
    TCP Offset:             5  (20 bytes)
    Reserved:               %0000
    TCP Flags:              %00011000  ...AP...
                               0... .... (No Congestion Window Reduction)
                               .0.. .... (No ECN-Echo)
                               ..0. .... (No Urgent pointer)
                               ...1 .... Ack
                               .... 1... Push
                               .... .0.. (No Reset)
                               .... ..0. (No SYN)
                               .... ...0 (No FIN)
    Window:                 7944
    TCP Checksum:           0xAD3B
    Urgent Pointer:         0
    No TCP Options
HTTP - Hyper Text Transfer Protocol
    HTTP Version:           HTTP/1.0
    HTTP Status:            200
    HTTP Reason:            OK<CR><LF>
    Server:                 Apache-Coyote/1.1<CR><LF>
    Content-Type:           text/html;charset=ISO-8859-1<CR><LF>
    Content-Language:       en-US<CR><LF>
    Content-Length:         534<CR><LF>
    Date:                   Mon, 08 Feb 2010 03:24:05 GMT<CR><LF>
    X-Cache:                MISS from 172.19.134.2<CR><LF>
    X-Cache-Lookup:         MISS from 172.19.134.2:3128<CR><LF>
    Via:                    1.0 172.19.134.2:3128 (squid/2.6.STABLE14)<CR><LF>
    Connection:             keep-alive<CR><LF><CR><LF>
    Line  1:                {<LF>
```



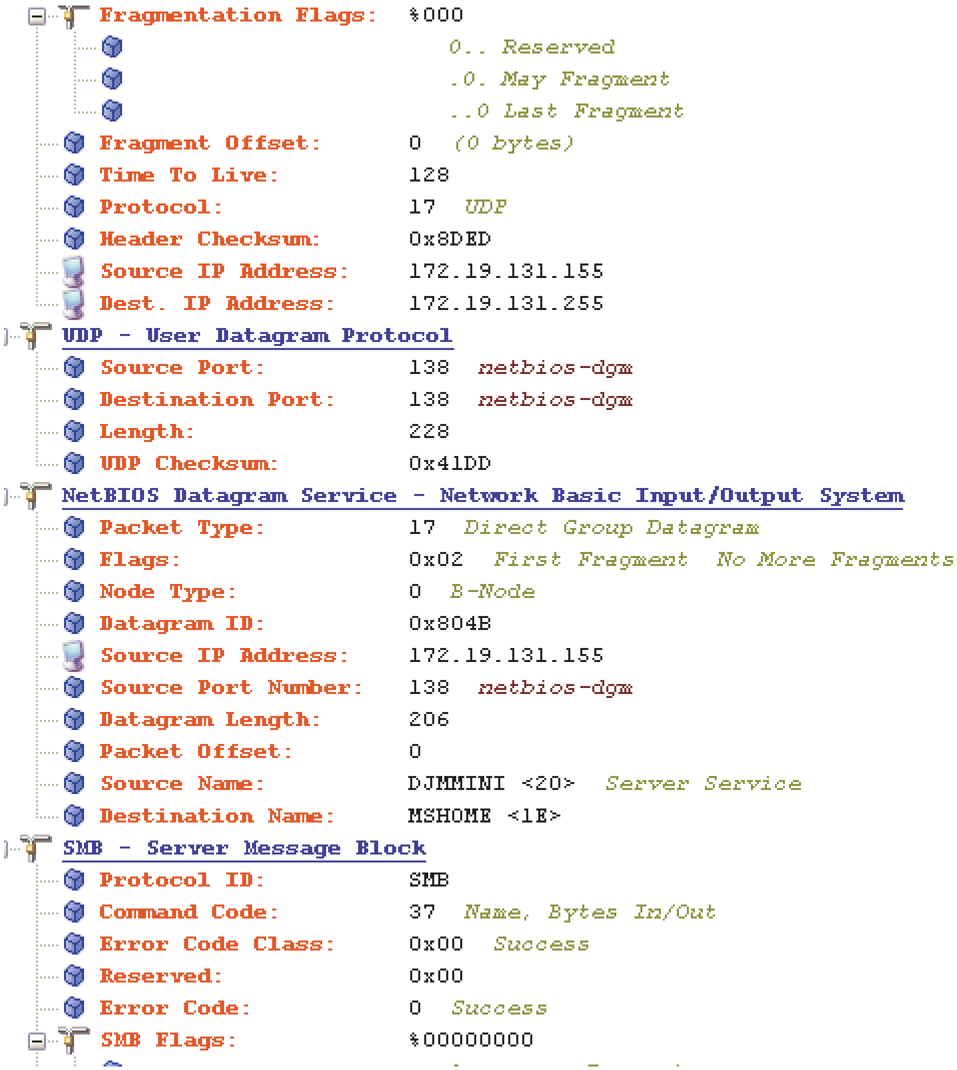
```
HOST_SERVICE:          FutureTenseContentServer:7.5.0<CR><LF>
Content-Type:          text/css<CR><LF>
Vary:                  Accept-Encoding<CR><LF>
Content-Encoding:      gzip<CR><LF>
Age:                   1375<CR><LF>
Content-Length:        8921<CR><LF>
X-Cache:               HIT from 172.19.134.2<CR><LF>
X-Cache-Lookup:        HIT from 172.19.134.2:3128<CR><LF>
Via:                   1.0 172.19.134.2:3128 (squid/2.6.STABLE14)<CR><LF>
Connection:            keep-alive<CR><LF><CR><LF><US><BS><NUL><NUL><NUL><NUL><NUL><NUL><ETX>
Binary Data:           (989 bytes)
FCS - Frame Check Sequence
FCS:                   0x52976E37   Calculated
```



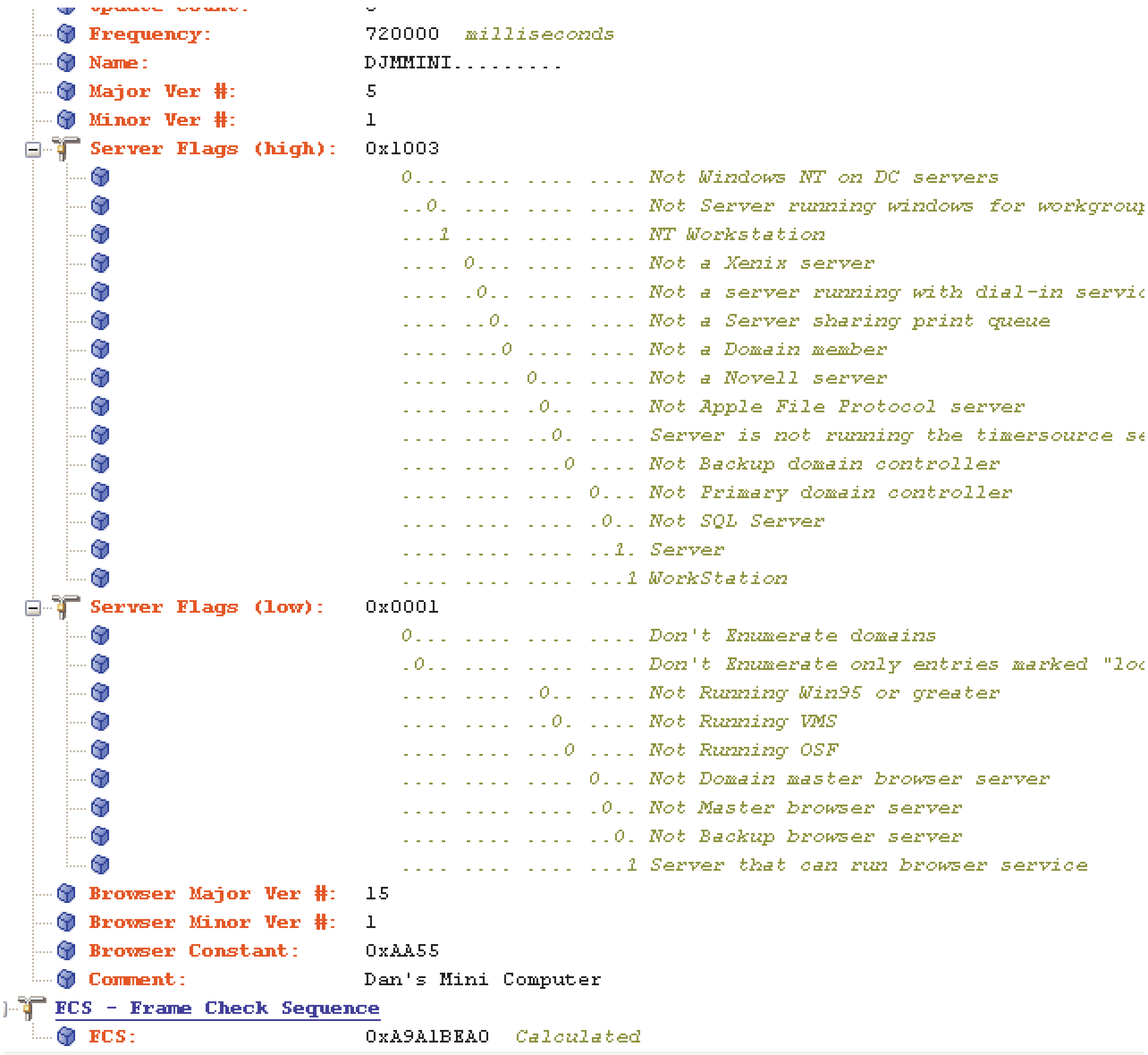
```
    Additional:            1
 Question
      Domain Name:          webmail.ccsainc.com
      Type:                 1  A - Host Address
      Class:                1  Internet
 Answer
      Domain Name:          webmail.ccsainc.com.    [Compressed Name]
      Type:                 1  A - Host Address
      Class:                1  Internet
      Time to Live:         7200
      Data Length:          4
      IP Address:           64.151.95.180
 Authority
      Domain Name:          ccsainc.com.    [Compressed Name]
      Type:                 2  NS - Authoritative Name Server
      Class:                1  Internet
      Time to Live:         172798
      Data Length:          16
      Domain Name:          ns47.worldnic.com.    [Compressed Name]
 Authority
      Domain Name:          ccsainc.com.    [Compressed Name]
      Type:                 2  NS - Authoritative Name Server
      Class:                1  Internet
      Time to Live:         172798
      Data Length:          7
      Domain Name:          ns48.worldnic.com.    [Compressed Name]
 Additional
      Domain Name:          ns48.worldnic.com.    [Compressed Name]
      Type:                 1  A - Host Address
      Class:                1  Internet
      Time to Live:         155622
      Data Length:          4
      IP Address:           205.178.144.24
FCS - Frame Check Sequence
```



```
    UDP Checksum:             0xF51E
NetBIOS Name Service - Network Basic Input/Output System
    Identification:           0x8028
    DNS Flags:                0x2910
                                 0... .... .... .... Query
                                 .010 1... .... .... Registration
                                 .... .0.. .... .... (Non-Authoritative Answer)
                                 .... ..0. .... .... (Message Not Truncated)
                                 .... ...1 .... .... Recursion Desired
                                 .... .... 0... .... (Recursion Not Available)
                                 .... .... .0.. .... (Reserved)
                                 .... .... ..0. .... (Authenticated Not Data)
                                 .... .... ...1 .... Checking Disabled
    Questions:                1
    Answers:                  0
    Authority:                0
    Additional:               1
    Question
        Domain Name:              DJMMINI <00>  Workstation
        Type:                     32  NetBIOS General Name Service
        Class:                    1  Internet
    Additional
        Domain Name:              DJMMINI <00>  Workstation    [Compressed Name]
        Type:                     32  NetBIOS General Name Service
        Class:                    1  Internet
        Time to Live:             300000
        Data Length:              6
        Resource Data
            Group Name Flag:          %0     is a UNIQUE NetBIOS name
            Owner Node Type:          %00     B node
            Reserved                  0     Must be zero
            Reserved                  0     Must be zero
            IP Address:               172.19.131.155
FCS - Frame Check Sequence
```



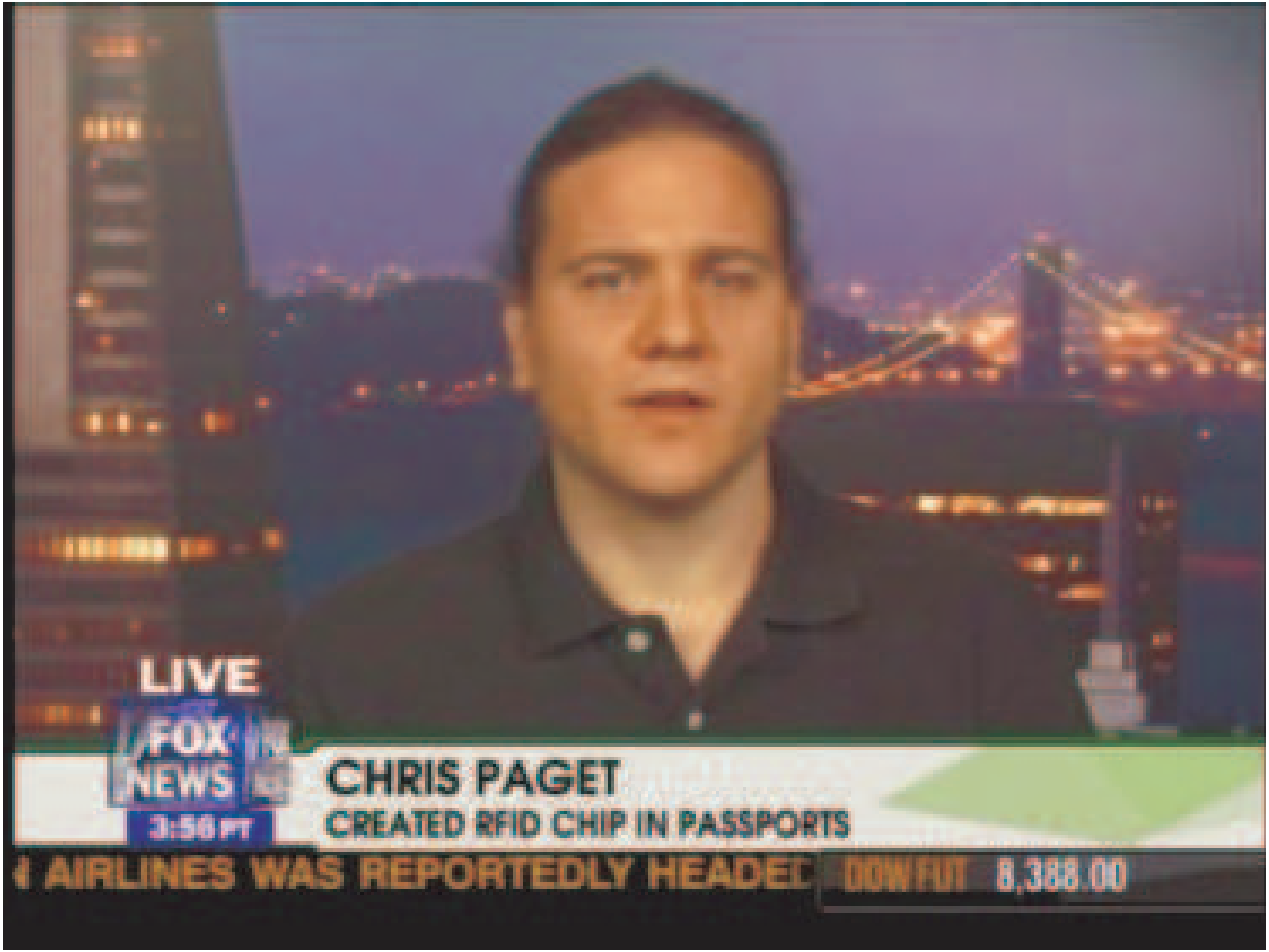
```
Fragmentation Flags:      %000
                               0.. Reserved
                               .0. May Fragment
                               ..0 Last Fragment
Fragment Offset:          0  (0 bytes)
Time To Live:             128
Protocol:                 17  UDP
Header Checksum:          0x8DED
Source IP Address:        172.19.131.155
Dest. IP Address:         172.19.131.255
UDP - User Datagram Protocol
Source Port:              138  netbios-dgm
Destination Port:         138  netbios-dgm
Length:                   228
UDP Checksum:             0x41DD
NetBIOS Datagram Service - Network Basic Input/Output System
Packet Type:              17  Direct Group Datagram
Flags:                    0x02  First Fragment  No More Fragments
Node Type:                0  B-Node
Datagram ID:              0x804B
Source IP Address:        172.19.131.155
Source Port Number:       138  netbios-dgm
Datagram Length:          206
Packet Offset:            0
Source Name:              DJMMINI <20>  Server Service
Destination Name:         MSHOME <1E>
SMB - Server Message Block
Protocol ID:              SMB
Command Code:             37  Name, Bytes In/Out
Error Code Class:         0x00  Success
Reserved:                 0x00
Error Code:               0  Success
SMB Flags:                %00000000
```

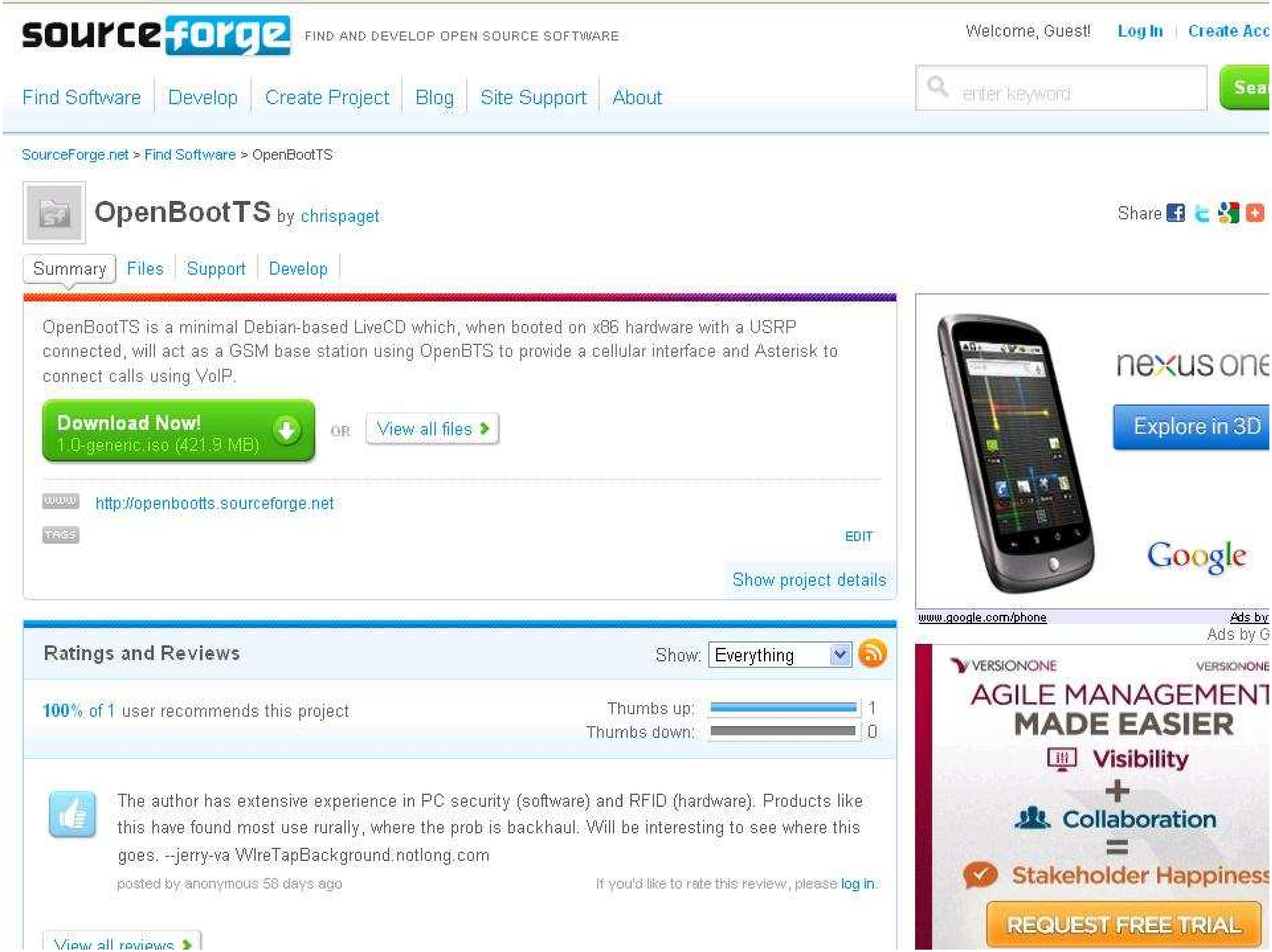


```
Update Count:              0
Frequency:                 720000  milliseconds
Name:                      DJMMINI.........
Major Ver #:               5
Minor Ver #:               1
Server Flags (high):       0x1003
                              0... .... .... .... Not Windows NT on DC servers
                              ..0. .... .... .... Not Server running windows for workgrou
                              ...1 .... .... .... NT Workstation
                              .... 0... .... .... Not a Xenix server
                              .... .0.. .... .... Not a server running with dial-in servi
                              .... ..0. .... .... Not a Server sharing print queue
                              .... ...0 .... .... Not a Domain member
                              .... .... 0... .... Not a Novell server
                              .... .... .0.. .... Not Apple File Protocol server
                              .... .... ..0. .... Server is not running the timersource se
                              .... .... ...0 .... Not Backup domain controller
                              .... .... .... 0... Not Primary domain controller
                              .... .... .... .0.. Not SQL Server
                              .... .... .... ..1. Server
                              .... .... .... ...1 WorkStation
Server Flags (low):        0x0001
                              0... .... .... .... Don't Enumerate domains
                              .0.. .... .... .... Don't Enumerate only entries marked "lo
                              .... .... .0.. .... Not Running Win95 or greater
                              .... .... ..0. .... Not Running VMS
                              .... .... ...0 .... Not Running OSF
                              .... .... .... 0... Not Domain master browser server
                              .... .... .... .0.. Not Master browser server
                              .... .... .... ..0. Not Backup browser server
                              .... .... .... ...1 Server that can run browser service
Browser Major Ver #:       15
Browser Minor Ver #:       1
Browser Constant:          0xAA55
Comment:                   Dan's Mini Computer
FCS - Frame Check Sequence
FCS:                       0xA9A1BEA0  Calculated
```

1855
SAMQQ CON

Virgin
21st AMENDMENT BREWERY
BREW FREE! OR DIE IPA


LIVE
FOX NEWS
3:56 PT
CHRIS PAGET
CREATED RFID CHIP IN PASSPORTS
AIRLINES WAS REPORTEDLY HEADED
DOW FUT 8,388.00



sourceforge
FIND AND DEVELOP OPEN SOURCE SOFTWARE
Welcome, Guest!
Log In | Create Acc
Find Software | Develop | Create Project | Blog | Site Support | About
enter keyword
Sea

SourceForge.net > Find Software > OpenBootTS

OpenBootTS by chrispaget

Share
Summary | Files | Support | Develop

OpenBootTS is a minimal Debian-based LiveCD which, when booted on x86 hardware with a USRP connected, will act as a GSM base station using OpenBTS to provide a cellular interface and Asterisk to connect calls using VoIP.

Download Now!
1.0-generic.iso (421.9 MB)
OR
View all files ›
www

http://openbootts.sourceforge.net

TAGS
EDIT
Show project details

Ratings and Reviews

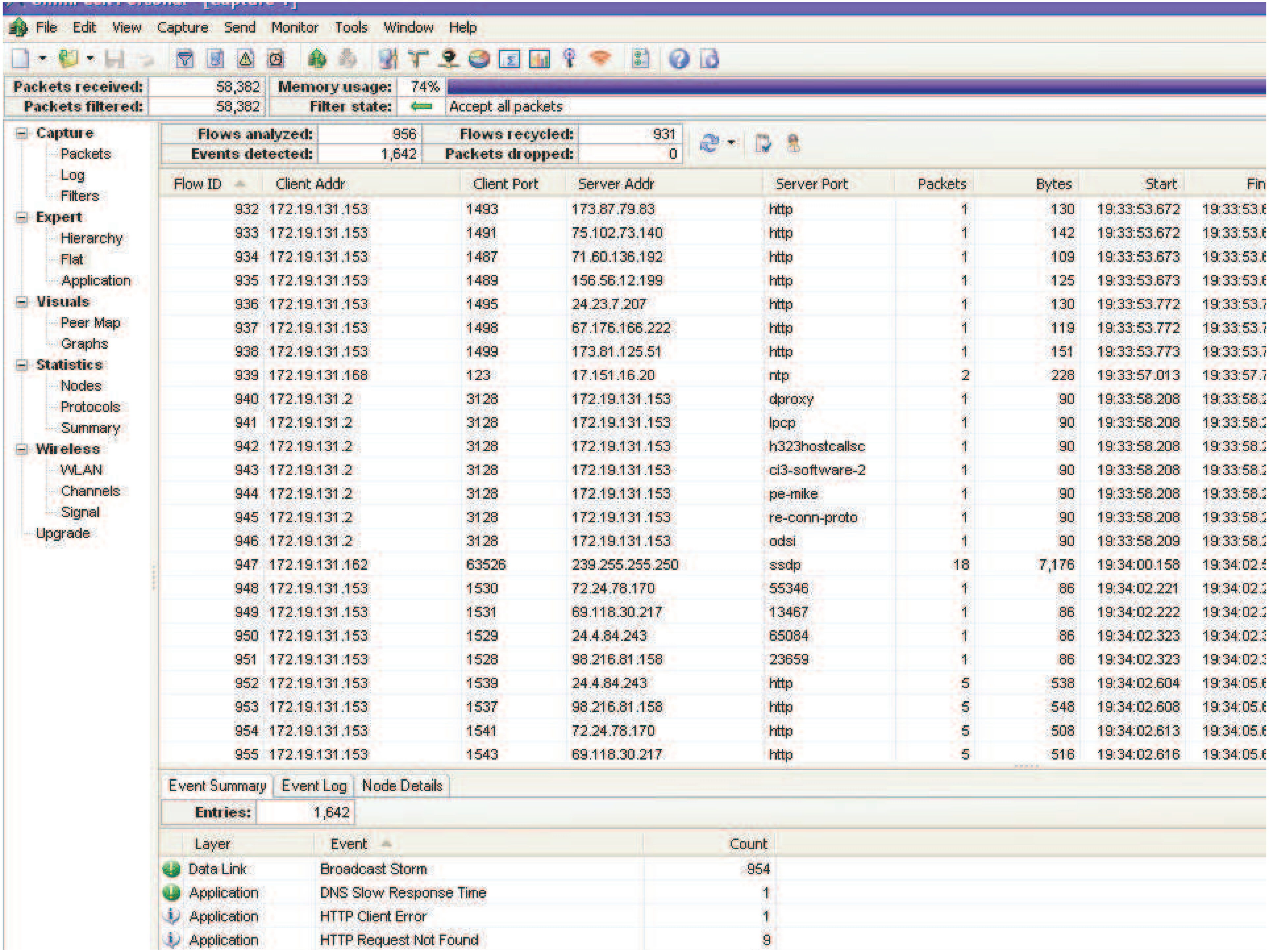
100% of 1 user recommends this project

Thumbs up: 1
Thumbs down: 0

The author has extensive experience in PC security (software) and RFID (hardware). Products like this have found most use rurally, where the prob is backhaul. Will be interesting to see where this goes. --jerry-va WIreTapBackground.notlong.com

posted by anonymous 58 days ago

If you'd like to rate this review, please log in.



Packets received: 58,382 **Memory usage:** 74%

Packets filtered: 58,382 **Filter state:** Accept all packets

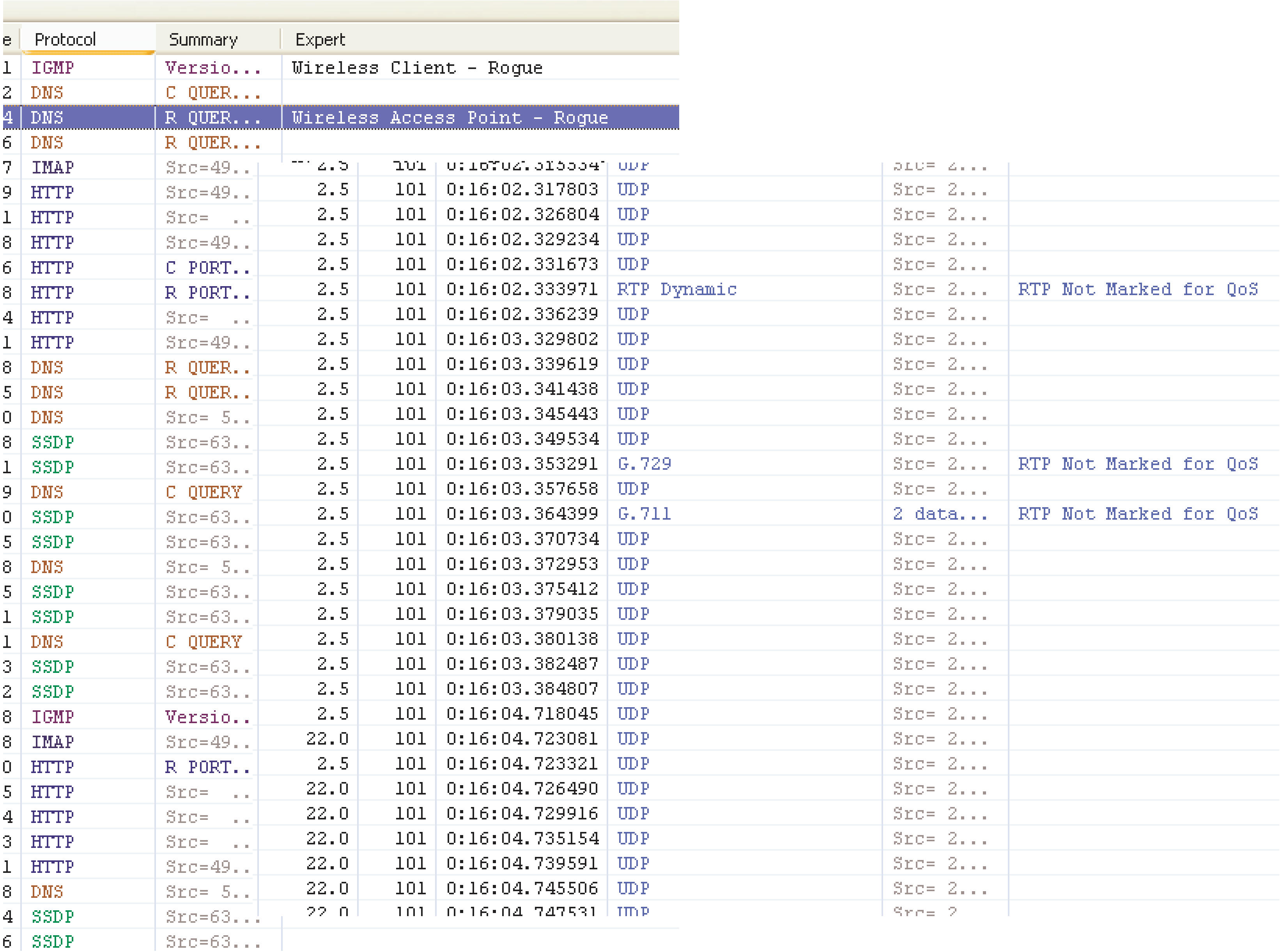
Flows analyzed: 956 **Flows recycled:** 931

Events detected: 1,642 **Packets dropped:** 0

Flow ID	Client Addr	Client Port	Server Addr	Server Port	Packets	Bytes	Start	Fin
932	172.19.131.153	1493	173.87.79.83	http	1	130	19:33:53.672	19:33:53.6
933	172.19.131.153	1491	75.102.73.140	http	1	142	19:33:53.672	19:33:53.6
934	172.19.131.153	1487	71.60.136.192	http	1	109	19:33:53.673	19:33:53.6
935	172.19.131.153	1489	156.56.12.199	http	1	125	19:33:53.673	19:33:53.6
936	172.19.131.153	1495	24.23.7.207	http	1	130	19:33:53.772	19:33:53.7
937	172.19.131.153	1498	67.176.166.222	http	1	119	19:33:53.772	19:33:53.7
938	172.19.131.153	1499	173.81.125.51	http	1	151	19:33:53.773	19:33:53.7
939	172.19.131.168	123	17.151.16.20	ntp	2	228	19:33:57.013	19:33:57.7
940	172.19.131.2	3128	172.19.131.153	dproxy	1	90	19:33:58.208	19:33:58.2
941	172.19.131.2	3128	172.19.131.153	lpcp	1	90	19:33:58.208	19:33:58.2
942	172.19.131.2	3128	172.19.131.153	h323hostcallsc	1	90	19:33:58.208	19:33:58.2
943	172.19.131.2	3128	172.19.131.153	ci3-software-2	1	90	19:33:58.208	19:33:58.2
944	172.19.131.2	3128	172.19.131.153	pe-mike	1	90	19:33:58.208	19:33:58.2
945	172.19.131.2	3128	172.19.131.153	re-conn-proto	1	90	19:33:58.208	19:33:58.2
946	172.19.131.2	3128	172.19.131.153	odsi	1	90	19:33:58.209	19:33:58.2
947	172.19.131.162	63526	239.255.255.250	ssdp	18	7,176	19:34:00.158	19:34:02.5
948	172.19.131.153	1530	72.24.78.170	55346	1	86	19:34:02.221	19:34:02.2
949	172.19.131.153	1531	69.118.30.217	13467	1	86	19:34:02.222	19:34:02.2
950	172.19.131.153	1529	24.4.84.243	65084	1	86	19:34:02.323	19:34:02.3
951	172.19.131.153	1528	98.216.81.158	23659	1	86	19:34:02.323	19:34:02.3
952	172.19.131.153	1539	24.4.84.243	http	5	538	19:34:02.604	19:34:05.6
953	172.19.131.153	1537	98.216.81.158	http	5	548	19:34:02.608	19:34:05.6
954	172.19.131.153	1541	72.24.78.170	http	5	508	19:34:02.613	19:34:05.6
955	172.19.131.153	1543	69.118.30.217	http	5	516	19:34:02.616	19:34:05.6

Entries: 1,642

Layer	Event	Count
Data Link	Broadcast Storm	954
Application	DNS Slow Response Time	1
Application	HTTP Client Error	1
Application	HTTP Request Not Found	9
]

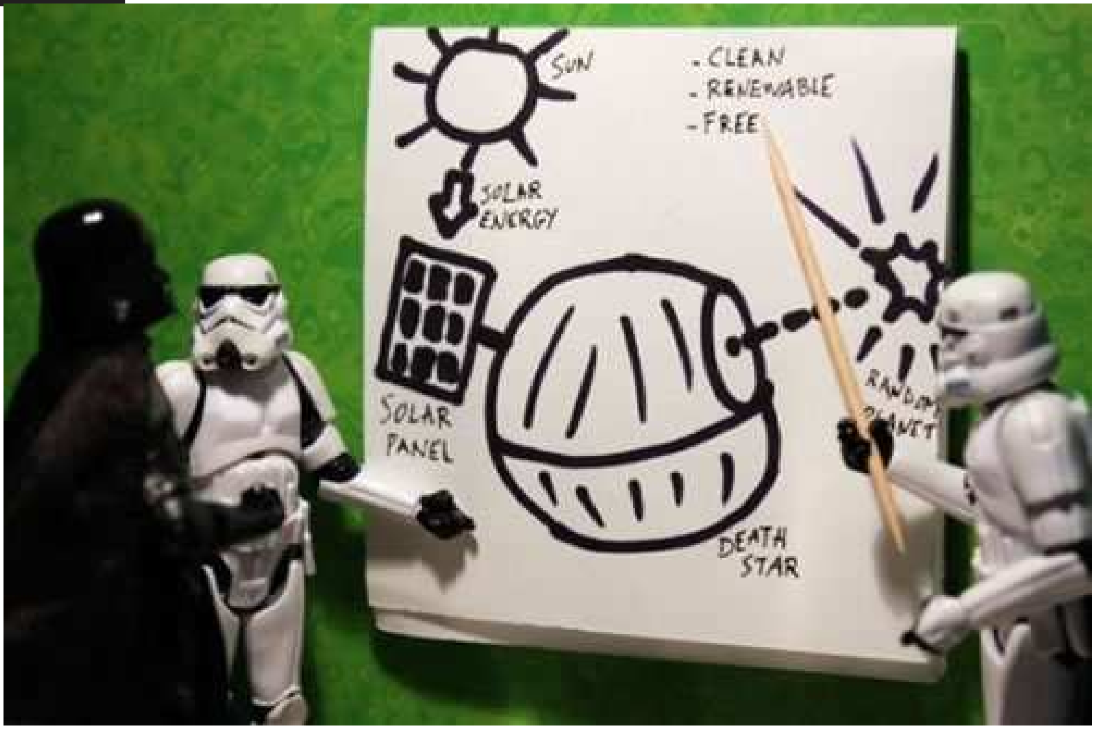


e	Protocol	Summary	Expert
1	IGMP	Versio...	Wireless Client - Rogue
2	DNS	C QUER...	
4	DNS	R QUER...	Wireless Access Point - Rogue
6	DNS	R QUER...	
7	IMAP	Src=49..	
9	HTTP	Src=49..	
1	HTTP	Src= ..	
8	HTTP	Src=49..	
6	HTTP	C PORT..	
8	HTTP	R PORT..	
4	HTTP	Src= ..	
1	HTTP	Src=49..	
8	DNS	R QUER..	
5	DNS	R QUER..	
0	DNS	Src= 5..	
8	SSDP	Src=63..	
1	SSDP	Src=63..	
9	DNS	C QUERY	
0	SSDP	Src=63..	
5	SSDP	Src=63..	
8	DNS	Src= 5..	
5	SSDP	Src=63..	
1	SSDP	Src=63..	
1	DNS	C QUERY	
3	SSDP	Src=63..	
2	SSDP	Src=63..	
8	IGMP	Versio..	
8	IMAP	Src=49..	
0	HTTP	R PORT..	
5	HTTP	Src= ..	
4	HTTP	Src= ..	
3	HTTP	Src= ..	
1	HTTP	Src=49..	
8	DNS	Src= 5..	
4	SSDP	Src=63...	
6	SSDP	Src=63...	

2.5	101	0:16:02.315334	UDP	Src= 2...	
2.5	101	0:16:02.317803	UDP	Src= 2...	
2.5	101	0:16:02.326804	UDP	Src= 2...	
2.5	101	0:16:02.329234	UDP	Src= 2...	
2.5	101	0:16:02.331673	UDP	Src= 2...	
2.5	101	0:16:02.333971	RTP Dynamic	Src= 2...	RTP Not Marked for QoS
2.5	101	0:16:02.336239	UDP	Src= 2...	
2.5	101	0:16:03.329802	UDP	Src= 2...	
2.5	101	0:16:03.339619	UDP	Src= 2...	
2.5	101	0:16:03.341438	UDP	Src= 2...	
2.5	101	0:16:03.345443	UDP	Src= 2...	
2.5	101	0:16:03.349534	UDP	Src= 2...	
2.5	101	0:16:03.353291	G.729	Src= 2...	RTP Not Marked for QoS
2.5	101	0:16:03.357658	UDP	Src= 2...	
2.5	101	0:16:03.364399	G.711	2 data...	RTP Not Marked for QoS
2.5	101	0:16:03.370734	UDP	Src= 2...	
2.5	101	0:16:03.372953	UDP	Src= 2...	
2.5	101	0:16:03.375412	UDP	Src= 2...	
2.5	101	0:16:03.379035	UDP	Src= 2...	
2.5	101	0:16:03.380138	UDP	Src= 2...	
2.5	101	0:16:03.382487	UDP	Src= 2...	
2.5	101	0:16:03.384807	UDP	Src= 2...	
2.5	101	0:16:04.718045	UDP	Src= 2...	
22.0	101	0:16:04.723081	UDP	Src= 2...	
2.5	101	0:16:04.723321	UDP	Src= 2...	
22.0	101	0:16:04.726490	UDP	Src= 2...	
22.0	101	0:16:04.729916	UDP	Src= 2...	
22.0	101	0:16:04.735154	UDP	Src= 2...	
22.0	101	0:16:04.739591	UDP	Src= 2...	
22.0	101	0:16:04.745506	UDP	Src= 2...	
22.0	101	0:16:04.747531	UDP	Src= 2	

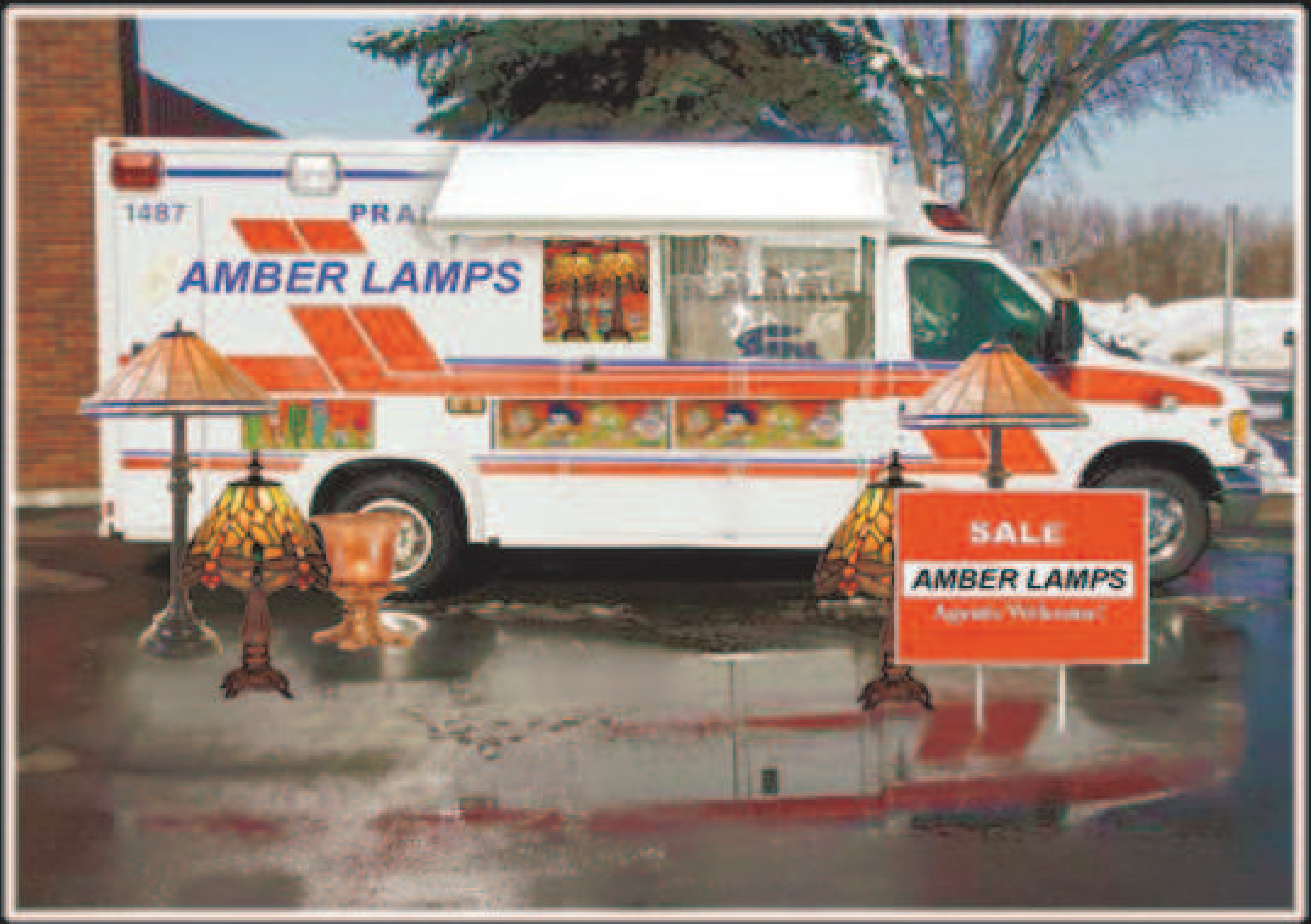
... along with

- Airdrop NG
- Dragorn's new tricks
- Windows 7 magic



CONCLUSION

- CAREFULL WITH TARGETED ATTACKS
  - CORPORATE ESPIONAGE
  - INTRA-COMPANY ESPIONAGE
- NOT THAT MANY BB DEVICES
- SOME TYPE OF "SIEM"-LIKE TOOL
  - PERSON'S NAME
  - USERNAME
  - MACHINE NAME
  - COMPANY NAME
  - IM
  - ETC



AMBER LAMPS

Bring them!

QUESTIONS?

THANKS

- @THOTCON
- @SPOOKERLABS
- @NELSONMURILO

CONTACT INFO:

@EFFFFN

LE(AT)YSTS.ORG

/LE(AT)DEFCONNETWORKING.ORG