```
No.     Time        Source                Destination           Protocol Length Info
   1797 7.684383    175.159.12.202        175.159.13.255        SSDP     434    NOTIFY * HTTP/1.1

Frame 1797: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits)
  Arrival Time: Nov 21, 2011 14:30:17.364070000 HKT
  Epoch Time: 1321857017.364070000 seconds
  [Time delta from previous captured frame: 0.000304000 seconds]
  [Time delta from previous displayed frame: 0.089445000 seconds]
  [Time since reference or first frame: 7.684383000 seconds]
  Frame Number: 1797
  Frame Length: 434 bytes (3472 bits)
  Capture Length: 434 bytes (3472 bits)
  [Frame is marked: True]
  [Frame is ignored: False]
  [Protocols in frame: eth:ip:udp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: IntelCor_5c:4f:b0 (00:26:c7:5c:4f:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
  Source: IntelCor_5c:4f:b0 (00:26:c7:5c:4f:b0)
    Address: IntelCor_5c:4f:b0 (00:26:c7:5c:4f:b0)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 175.159.12.202 (175.159.12.202), Dst: 175.159.13.255 (175.159.13.255)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x60 (DSCP 0x18: Class Selector 3; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0110 00.. = Differentiated Services Codepoint: Class Selector 3 (0x18)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 420
  Identification: 0x4bb3 (19379)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don’t fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0xb32e [correct]
    [Good: True]
    [Bad: False]
  Source: 175.159.12.202 (175.159.12.202)
  Destination: 175.159.13.255 (175.159.13.255)
User Datagram Protocol, Src Port: ssdp (1900), Dst Port: fjicl-tep-a (1901)
  Source port: ssdp (1900)
  Destination port: fjicl-tep-a (1901)
  Length: 400
  Checksum: 0xa3ac [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
Hypertext Transfer Protocol
  NOTIFY * HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): NOTIFY * HTTP/1.1\r\n]
      [Message: NOTIFY * HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: NOTIFY
    Request URI: *
    Request Version: HTTP/1.1
  HOST: 175.159.13.255:1901\r\n
  SERVER: Windows XP SP3/5.1.2600 IKU/2.1 Center/1.0.1.0\r\n
  CACHE-CONTROL: max-age=100\r\n
  LOCATION: http://175.159.12.202:8909/upnp/iKuCenterServices.xml\r\n
  NTS: ssdp:alive\r\n
  LAST-UPDATED-TIME: 1407\r\n
```

```
    NT: urn:schemas-iku-yoku-com:service:RemoteControl:1\r\n
    USN: uuid:060b735a-fcac-4466-8909-1fbfb9add62c::urn:schemas-iku-youku-com:service:RemoteControl:1\r\n
    \r\n
    [Full request URI: http://175.159.13.255:1901*]

0000  ff ff ff ff ff ff 00 26 c7 5c 4f b0 08 00 45 60   .......&.\O...E‘
0010  01 a4 4b b3 00 00 40 11 b3 2e af 9f 0c ca af 9f   ..K...@.........
0020  0d ff 07 6c 07 6d 01 90 a3 ac 4e 4f 54 49 46 59   ...l.m....NOTIFY
0030  20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 4f 53    * HTTP/1.1..HOS
0040  54 3a 20 31 37 35 2e 31 35 39 2e 31 33 2e 32 35   T: 175.159.13.25
0050  35 3a 31 39 30 31 0d 0a 53 45 52 56 45 52 3a 20   5:1901..SERVER: 
0060  57 69 6e 64 6f 77 73 20 58 50 20 53 50 33 2f 35   Windows XP SP3/5
0070  2e 31 2e 32 36 30 30 20 49 4b 55 2f 32 2e 31 20   .1.2600 IKU/2.1 
0080  43 65 6e 74 65 72 2f 31 2e 30 2e 31 2e 30 0d 0a   Center/1.0.1.0..
0090  43 41 43 48 45 2d 43 4f 4e 54 52 4f 4c 3a 20 6d   CACHE-CONTROL: m
00a0  61 78 2d 61 67 65 3d 31 30 30 0d 0a 4c 4f 43 41   ax-age=100..LOCA
00b0  54 49 4f 4e 3a 20 68 74 74 70 3a 2f 2f 31 37 35   TION: http://175
00c0  2e 31 35 39 2e 31 32 2e 32 30 32 3a 38 39 30 39   .159.12.202:8909
00d0  2f 75 70 6e 70 2f 69 4b 75 43 65 6e 74 65 72 53   /upnp/iKuCenterS
00e0  65 72 76 69 63 65 73 2e 78 6d 6c 0d 0a 4e 54 53   ervices.xml..NTS
00f0  3a 20 73 73 64 70 3a 61 6c 69 76 65 0d 0a 4c 41   : ssdp:alive..LA
0100  53 54 2d 55 50 44 41 54 45 44 2d 54 49 4d 45 3a   ST-UPDATED-TIME:
0110  20 31 34 30 37 0d 0a 4e 54 3a 20 75 72 6e 3a 73    1407..NT: urn:s
0120  63 68 65 6d 61 73 2d 69 6b 75 2d 79 6f 6b 75 2d   chemas-iku-yoku-
0130  63 6f 6d 3a 73 65 72 76 69 63 65 3a 52 65 6d 6f   com:service:Remo
0140  74 65 43 6f 6e 74 72 6f 6c 3a 31 0d 0a 55 53 4e   teControl:1..USN
0150  3a 20 75 75 69 64 3a 30 36 30 62 37 33 35 61 2d   : uuid:060b735a-
0160  66 63 61 63 2d 34 34 36 36 2d 38 39 30 39 2d 31   fcac-4466-8909-1
0170  66 62 66 62 39 61 64 64 36 32 63 3a 3a 75 72 6e   fbfb9add62c::urn
0180  3a 73 63 68 65 6d 61 73 2d 69 6b 75 2d 79 6f 75   :schemas-iku-you
0190  6b 75 2d 63 6f 6d 3a 73 65 72 76 69 63 65 3a 52   ku-com:service:R
01a0  65 6d 6f 74 65 43 6f 6e 74 72 6f 6c 3a 31 0d 0a   emoteControl:1..
01b0  0d 0a                                             ..
```

```
No.     Time        Source                Destination           Protocol Length Info
   2039 8.776157    128.119.245.12        175.159.28.97         HTTP     446    [TCP Retransmission] HTTP/1.1 20
0 OK  (text/html)

Frame 2039: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits)
  Arrival Time: Nov 21, 2011 14:30:18.455844000 HKT
  Epoch Time: 1321857018.455844000 seconds
  [Time delta from previous captured frame: 0.040823000 seconds]
  [Time delta from previous displayed frame: 0.040851000 seconds]
  [Time since reference or first frame: 8.776157000 seconds]
  Frame Number: 2039
  Frame Length: 446 bytes (3568 bits)
  Capture Length: 446 bytes (3568 bits)
  [Frame is marked: True]
  [Frame is ignored: False]
  [Protocols in frame: eth:ip:tcp:http:data-text-lines]
  [Coloring Rule Name: Bad TCP]
  [Coloring Rule String: tcp.analysis.flags]
Ethernet II, Src: Cisco_b8:cc:80 (00:0f:f8:b8:cc:80), Dst: 28:37:37:18:f5:76 (28:37:37:18:f5:76)
  Destination: 28:37:37:18:f5:76 (28:37:37:18:f5:76)
    Address: 28:37:37:18:f5:76 (28:37:37:18:f5:76)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  Source: Cisco_b8:cc:80 (00:0f:f8:b8:cc:80)
    Address: Cisco_b8:cc:80 (00:0f:f8:b8:cc:80)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 175.159.28.97 (175.159.28.97)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 432
  Identification: 0xaa5c (43612)
  Flags: 0x02 (Don’t Fragment)
    0... .... = Reserved bit: Not set
    .1.. .... = Don’t fragment: Set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 49
  Protocol: TCP (6)
  Header checksum: 0x5c67 [correct]
    [Good: True]
    [Bad: False]
  Source: 128.119.245.12 (128.119.245.12)
  Destination: 175.159.28.97 (175.159.28.97)
Transmission Control Protocol, Src Port: http (80), Dst Port: 49673 (49673), Seq: 1, Ack: 412, Len: 380
  Source port: http (80)
  Destination port: 49673 (49673)
  [Stream index: 100]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 381    (relative sequence number)]
  Acknowledgement number: 412    (relative ack number)
  Header length: 32 bytes
  Flags: 0x18 (PSH, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgement: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 54
  [Calculated window size: 6912]
  [Window size scaling factor: 128]
  Checksum: 0x7810 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes)
    No-Operation (NOP)
    No-Operation (NOP)
    Timestamps: TSval 1860405412, TSecr 1059930312
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 1860405412
      Timestamp echo reply: 1059930312
  [SEQ/ACK analysis]
    [Bytes in flight: 380]
    [TCP Analysis Flags]
      [This frame is a (suspected) retransmission]
        [Expert Info (Note/Sequence): Retransmission (suspected)]
          [Message: Retransmission (suspected)]
          [Severity level: Note]
          [Group: Sequence]
      [The RTO for this segment was: 0.956178000 seconds]
      [RTO based on delta from frame: 1825]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [Message: HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 200
    Response Phrase: OK
  Date: Mon, 21 Nov 2011 06:30:05 GMT\r\n
  Server: Apache/2.2.3 (CentOS)\r\n
  Last-Modified: Mon, 21 Nov 2011 06:30:01 GMT\r\n
  ETag: "8734b-51-d0fd0c40"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 81\r\n
    [Content length: 81]
  Keep-Alive: timeout=10, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
Line-based text data: text/html
  <html>\n
  Congratulations!  You’ve downloaded the first Wireshark lab file!\n
  </html>\n

0000  28 37 37 18 f5 76 00 0f f8 b8 cc 80 08 00 45 00   (77..v........E.
0010  01 b0 aa 5c 40 00 31 06 5c 67 80 77 f5 0c af 9f   ...\@.1.\g.w....
0020  1c 61 00 50 c2 09 51 2f 2e bc f8 7b a6 47 80 18   .a.P..Q/...{.G..
0030  00 36 78 10 00 00 01 01 08 0a 6e e3 88 a4 3f 2d   .6x.......n...?-
0040  40 c8 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f   @.HTTP/1.1 200 O
0050  4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 32 31   K..Date: Mon, 21
0060  20 4e 6f 76 20 32 30 31 31 20 30 36 3a 33 30 3a    Nov 2011 06:30:
0070  30 35 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20   05 GMT..Server: 
0080  41 70 61 63 68 65 2f 32 2e 32 2e 33 20 28 43 65   Apache/2.2.3 (Ce
0090  6e 74 4f 53 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69   ntOS)..Last-Modi
00a0  66 69 65 64 3a 20 4d 6f 6e 2c 20 32 31 20 4e 6f   fied: Mon, 21 No
00b0  76 20 32 30 31 31 20 30 36 3a 33 30 3a 30 31 20   v 2011 06:30:01 
00c0  47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 37 33 34   GMT..ETag: "8734
00d0  62 2d 35 31 2d 64 30 66 64 30 63 34 30 22 0d 0a   b-51-d0fd0c40"..
00e0  41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62   Accept-Ranges: b
00f0  79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65   ytes..Content-Le
0100  6e 67 74 68 3a 20 38 31 0d 0a 4b 65 65 70 2d 41   ngth: 81..Keep-A
0110  6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 31 30   live: timeout=10
0120  2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65   , max=100..Conne
0130  63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76   ction: Keep-Aliv
0140  65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a   e..Content-Type:
0150  20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72    text/html; char
0160  73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74   set=UTF-8....<ht
0170  6d 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69   ml>.Congratulati
```

```
0180  6f 6e 73 21 20 20 59 6f 75 27 76 65 20 64 6f 77   ons!  You’ve dow
0190  6e 6c 6f 61 64 65 64 20 74 68 65 20 66 69 72 73   nloaded the firs
01a0  74 20 57 69 72 65 73 68 61 72 6b 20 6c 61 62 20   t Wireshark lab 
01b0  66 69 6c 65 21 0a 3c 2f 68 74 6d 6c 3e 0a         file!.</html>.
```