```
No.     Time               Source                Destination           Protocol Length Info
    253 22:56:38.262749    128.119.245.12        192.168.1.193         HTTP     831    HTTP/1.1 200 OK  (text/html)
Frame 253: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface 0
    Interface id: 0 (\Device\NPF_{DD9A2CBB-790F-4E1B-9193-676A762F8E4D})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 18, 2019 22:56:38.262749000 Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1550548598.262749000 seconds
    [Time delta from previous captured frame: 0.000002000 seconds]
    [Time delta from previous displayed frame: 0.076780000 seconds]
    [Time since reference or first frame: 10.912749000 seconds]
    Frame Number: 253
    Frame Length: 831 bytes (6648 bits)
    Capture Length: 831 bytes (6648 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: VerizonB_bd:79:42 (c8:a7:0a:bd:79:42), Dst: IntelCor_53:6f:24 (f8:63:3f:53:6f:24)
    Destination: IntelCor_53:6f:24 (f8:63:3f:53:6f:24)
    Source: VerizonB_bd:79:42 (c8:a7:0a:bd:79:42)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.193
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 817
    Identification: 0x4efa (20218)
    Flags: 0x4000, Don't fragment
    Time to live: 53
    Protocol: TCP (6)
    Header checksum: 0xbbdf [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 192.168.1.193
Transmission Control Protocol, Src Port: 80, Dst Port: 56415, Seq: 1, Ack: 152938, Len: 777
    Source Port: 80
    Destination Port: 56415
    [Stream index: 5]
    [TCP Segment Len: 777]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 778    (relative sequence number)]
    Acknowledgment number: 152938    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 1432
    [Calculated window size: 183296]
    [Window size scaling factor: 128]
    Checksum: 0x863b [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (777 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 19 Feb 2019 03:56:36 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sat, 23 Oct 2010 11:38:58 GMT\r\n
    ETag: "1a2-4934734677880"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 418\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.076780000 seconds]
    [Request in frame: 211]
    File Data: 418 bytes
Line-based text data: text/html (11 lines)
    <TITLE>Upload page for TCP Ethereal Lab</TITLE>\n
    <body bgcolor="#FFFFFF">\n
    <p><font face="Arial, Helvetica, sans-serif" size="4"> Congratulations! <br> </font>\n
    \n
    <P><font face="Arial, Helvetica, sans-serif"> You've now transferred a copy of alice.txt ffrom\n
    your computer to \n
    gaia.cs.umass.edu.  You should now stop Wireshark packet capture. It's time to start analyzing the captured Wireshark packets! </font>
\n
    \n
    </FORM>\n
```

\n
\n