```
No.     Time           Source                Destination           Protocol Length Info
   3430 56.761739000   10.0.1.51             171.66.3.23           HTTP     221    GET /token?keywords=java&app_
id=9469ea8ba22b4786f382986111518038 HTTP/1.1

Frame 3430: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:18:01.793159000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340281.793159000 seconds
  [Time delta from previous captured frame: 0.031403000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 56.761739000 seconds]
  Frame Number: 3430
  Frame Length: 221 bytes (1768 bits)
  Capture Length: 221 bytes (1768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 205
  Identification: 0xba6c (47724)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0xc632 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60583 (60583), Dst Port: http (80), Seq: 1, Ack: 1, Len: 153
  Source port: 60583 (60583)
  Destination port: http (80)
  [Stream index: 138]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 154    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0x6206 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16434747, TSecr 54374838
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16434747
      Timestamp echo reply: 54374838
  [SEQ/ACK analysis]
    [Bytes in flight: 153]
Hypertext Transfer Protocol
  GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Message: GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: Keep-Alive\r\n
  User-Agent: adlib-android\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/token?keywords=java&app_id=9469ea8ba22b4786f382986111518038]
```

```
No.     Time           Source                Destination           Protocol Length Info
   3434 56.777063000   171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 3434: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:18:01.808483000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340281.808483000 seconds
  [Time delta from previous captured frame: 0.000496000 seconds]
  [Time delta from previous displayed frame: 0.015324000 seconds]
  [Time since reference or first frame: 56.777063000 seconds]
  Frame Number: 3434
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xb7f2 (47090)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x1621 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60583 (60583), Seq: 279, Ack: 154, Len: 5
  Source port: http (80)
  Destination port: 60583 (60583)
  [Stream index: 138]
  Sequence number: 279    (relative sequence number)
  [Next sequence number: 284    (relative sequence number)]
  Acknowledgment number: 154    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0xd1d8 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54374852, TSecr 16434747
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54374852
      Timestamp echo reply: 16434747
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (283 bytes): #3432(278), #3434(5)]
  [Frame: 3432, payload: 0-277 (278 bytes)]
  [Frame: 3434, payload: 278-282 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 283]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:18:58 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (118 octets)
      Chunk size: 118 octets
      Data (118 bytes)

0000  3c 61 20 68 72 65 66 3d 22 2f 63 6c 69 63 6b 2f   <a href="/click/
0010  64 65 66 63 35 30 35 64 34 38 38 65 30 61 30 30   defc505d488e0a00
0020  66 66 39 32 66 37 62 30 61 63 31 63 33 38 63 37   ff92f7b0ac1c38c7
0030  2f 34 39 34 61 30 36 35 61 36 61 66 62 36 34 63   /494a065a6afb64c
0040  33 33 33 34 38 63 32 34 39 64 61 32 62 66 35 35   33348c249da2bf55
0050  62 22 3e 43 6c 69 63 6b 20 68 65 72 65 20 74 6f   b">Click here to
0060  20 77 69 6e 20 24 31 30 30 2c 30 30 30 2c 30 30    win $100,000,00
0070  30 21 3c 2f 61 3e                                 0!</a>
        Data: 3c6120687265663d222f636c69636b2f6465666335303564...
        [Length: 118]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <a href="/click/defc505d488e0a00ff92f7b0ac1c38c7/494a065a6afb64c33348c249da2bf55b">Click here to win $100,000,00
  0!</a>
```

```
No.     Time           Source                Destination           Protocol Length Info
   3740 101.829588000  10.0.1.51             171.66.3.23           HTTP     221    GET /token?keywords=java&app_
id=9469ea8ba22b4786f382986111518038 HTTP/1.1

Frame 3740: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:18:46.861008000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340326.861008000 seconds
  [Time delta from previous captured frame: 0.105940000 seconds]
  [Time delta from previous displayed frame: 45.052525000 seconds]
  [Time since reference or first frame: 101.829588000 seconds]
  Frame Number: 3740
  Frame Length: 221 bytes (1768 bits)
  Capture Length: 221 bytes (1768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 205
  Identification: 0xa22e (41518)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0xde70 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60599 (60599), Dst Port: http (80), Seq: 1, Ack: 1, Len: 153
  Source port: 60599 (60599)
  Destination port: http (80)
  [Stream index: 155]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 154    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0x76d0 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16448268, TSecr 54388328
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16448268
      Timestamp echo reply: 54388328
  [SEQ/ACK analysis]
    [Bytes in flight: 153]
Hypertext Transfer Protocol
  GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Message: GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: Keep-Alive\r\n
  User-Agent: adlib-android\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/token?keywords=java&app_id=9469ea8ba22b4786f382986111518038]
```

```
No.     Time           Source                Destination           Protocol Length Info
   3744 101.851820000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 3744: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:18:46.883240000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340326.883240000 seconds
  [Time delta from previous captured frame: 0.003735000 seconds]
  [Time delta from previous displayed frame: 0.022232000 seconds]
  [Time since reference or first frame: 101.851820000 seconds]
  Frame Number: 3744
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xfe7d (65149)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0xcf95 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60599 (60599), Seq: 279, Ack: 154, Len: 5
  Source port: http (80)
  Destination port: 60599 (60599)
  [Stream index: 155]
  Sequence number: 279    (relative sequence number)
  [Next sequence number: 284    (relative sequence number)]
  Acknowledgment number: 154    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0xe683 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54388373, TSecr 16448268
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54388373
      Timestamp echo reply: 16448268
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (283 bytes): #3742(278), #3744(5)]
  [Frame: 3742, payload: 0-277 (278 bytes)]
  [Frame: 3744, payload: 278-282 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 283]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:19:43 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (118 octets)
      Chunk size: 118 octets
      Data (118 bytes)

0000  3c 61 20 68 72 65 66 3d 22 2f 63 6c 69 63 6b 2f   <a href="/click/
0010  64 65 66 63 35 30 35 64 34 38 38 65 30 61 30 30   defc505d488e0a00
0020  66 66 39 32 66 37 62 30 61 63 31 63 33 38 63 37   ff92f7b0ac1c38c7
0030  2f 39 30 61 66 32 35 64 61 36 63 30 32 61 34 36   /90af25da6c02a46
0040  39 32 34 38 38 36 37 37 38 30 64 32 32 34 66 36   9248867780d224f6
0050  65 22 3e 43 6c 69 63 6b 20 68 65 72 65 20 74 6f   e">Click here to
0060  20 77 69 6e 20 24 31 30 30 2c 30 30 30 2c 30 30    win $100,000,00
0070  30 21 3c 2f 61 3e                                 0!</a>
        Data: 3c6120687265663d222f636c69636b2f6465666335303564...
        [Length: 118]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <a href="/click/defc505d488e0a00ff92f7b0ac1c38c7/90af25da6c02a469248867780d224f6e">Click here to win $100,000,00
  0!</a>
```

```
No.     Time           Source                Destination           Protocol Length Info
   3871 121.507272000  10.0.1.51             171.66.3.23           HTTP     221    GET /token?keywords=java&app_
id=9469ea8ba22b4786f382986111518038 HTTP/1.1

Frame 3871: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:06.538692000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340346.538692000 seconds
  [Time delta from previous captured frame: 0.061585000 seconds]
  [Time delta from previous displayed frame: 19.655452000 seconds]
  [Time since reference or first frame: 121.507272000 seconds]
  Frame Number: 3871
  Frame Length: 221 bytes (1768 bits)
  Capture Length: 221 bytes (1768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 205
  Identification: 0xdc6c (56428)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0xa432 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60607 (60607), Dst Port: http (80), Seq: 1, Ack: 1, Len: 153
  Source port: 60607 (60607)
  Destination port: http (80)
  [Stream index: 163]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 154    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0x2c08 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16454171, TSecr 54394233
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16454171
      Timestamp echo reply: 54394233
  [SEQ/ACK analysis]
    [Bytes in flight: 153]
Hypertext Transfer Protocol
  GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Message: GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: Keep-Alive\r\n
  User-Agent: adlib-android\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/token?keywords=java&app_id=9469ea8ba22b4786f382986111518038]
```

```
No.     Time           Source                Destination           Protocol Length Info
   3875 121.525258000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 3875: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:06.556678000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340346.556678000 seconds
  [Time delta from previous captured frame: 0.000419000 seconds]
  [Time delta from previous displayed frame: 0.017986000 seconds]
  [Time since reference or first frame: 121.525258000 seconds]
  Frame Number: 3875
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x616e (24942)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x6ca5 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60607 (60607), Seq: 279, Ack: 154, Len: 5
  Source port: http (80)
  Destination port: 60607 (60607)
  [Stream index: 163]
  Sequence number: 279    (relative sequence number)
  [Next sequence number: 284    (relative sequence number)]
  Acknowledgment number: 154    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0x9bbd [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54394276, TSecr 16454171
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54394276
      Timestamp echo reply: 16454171
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (283 bytes): #3873(278), #3875(5)]
  [Frame: 3873, payload: 0-277 (278 bytes)]
  [Frame: 3875, payload: 278-282 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 283]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:02 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (118 octets)
      Chunk size: 118 octets
      Data (118 bytes)

0000  3c 61 20 68 72 65 66 3d 22 2f 63 6c 69 63 6b 2f   <a href="/click/
0010  64 65 66 63 35 30 35 64 34 38 38 65 30 61 30 30   defc505d488e0a00
0020  66 66 39 32 66 37 62 30 61 63 31 63 33 38 63 37   ff92f7b0ac1c38c7
0030  2f 38 33 38 37 37 34 36 32 30 30 30 33 65 66 63   /838774620003efc
0040  62 39 63 39 64 33 61 33 63 65 32 66 34 66 65 35   b9c9d3a3ce2f4fe5
0050  33 22 3e 43 6c 69 63 6b 20 68 65 72 65 20 74 6f   3">Click here to
0060  20 77 69 6e 20 24 31 30 30 2c 30 30 30 2c 30 30    win $100,000,00
0070  30 21 3c 2f 61 3e                                 0!</a>
      Data: 3c6120687265663d222f636c69636b2f6465666335303564...
      [Length: 118]
    Chunk boundary
  End of chunked encoding
    Chunk size: 0 octets
    Chunk boundary
Line-based text data: text/html
  <a href="/click/defc505d488e0a00ff92f7b0ac1c38c7/838774620003efcb9c9d3a3ce2f4fe53">Click here to win $100,000,00
  0!</a>
```

```
No.     Time           Source                Destination           Protocol Length Info
   4079 125.744543000  10.0.1.51             171.66.3.23           HTTP     582    GET /click/defc505d488e0a00ff
92f7b0ac1c38c7/838774620003efcb9c9d3a3ce2f4fe53 HTTP/1.1

Frame 4079: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:10.775963000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340350.775963000 seconds
  [Time delta from previous captured frame: 0.015187000 seconds]
  [Time delta from previous displayed frame: 4.219285000 seconds]
  [Time since reference or first frame: 125.744543000 seconds]
  Frame Number: 4079
  Frame Length: 582 bytes (4656 bits)
  Capture Length: 582 bytes (4656 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 566
  Identification: 0x4cdd (19677)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x3259 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 1, Ack: 1, Len: 514
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 515    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0x70c5 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16455442, TSecr 54395538
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16455442
      Timestamp echo reply: 54395538
  [SEQ/ACK analysis]
    [Bytes in flight: 514]
Hypertext Transfer Protocol
  GET /click/defc505d488e0a00ff92f7b0ac1c38c7/838774620003efcb9c9d3a3ce2f4fe53 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /click/defc505d488e0a00ff92f7b0ac1c38c7/838774620003efcb9c9d3a3ce2f4fe53 HTTP/
    1.1\r\n]
      [Message: GET /click/defc505d488e0a00ff92f7b0ac1c38c7/838774620003efcb9c9d3a3ce2f4fe53 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /click/defc505d488e0a00ff92f7b0ac1c38c7/838774620003efcb9c9d3a3ce2f4fe53
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/838774620003efcb9c9d3a3ce2f4f
  e53]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4083 125.763876000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 4083: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:10.795296000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340350.795296000 seconds
  [Time delta from previous captured frame: 0.000973000 seconds]
  [Time delta from previous displayed frame: 0.019333000 seconds]
  [Time since reference or first frame: 125.763876000 seconds]
  Frame Number: 4083
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x2107 (8455)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0xad0c [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 168, Ack: 515, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 168    (relative sequence number)
  [Next sequence number: 173    (relative sequence number)]
  Acknowledgment number: 515    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0x810c [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54395547, TSecr 16455442
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54395547
      Timestamp echo reply: 16455442
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (172 bytes): #4081(167), #4083(5)]
  [Frame: 4081, payload: 0-166 (167 bytes)]
  [Frame: 4083, payload: 167-171 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 172]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:06 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (8 octets)
      Chunk size: 8 octets
      Data (8 bytes)

0000  53 75 63 63 65 73 73 21                           Success!
        Data: 5375636365737321
        [Length: 8]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  Success!
```

```
No.     Time           Source                Destination           Protocol Length Info
   4085 125.913390000  10.0.1.51             171.66.3.23           HTTP     556    GET /favicon.ico HTTP/1.1

Frame 4085: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:10.944810000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340350.944810000 seconds
  [Time delta from previous captured frame: 0.149508000 seconds]
  [Time delta from previous displayed frame: 0.149514000 seconds]
  [Time since reference or first frame: 125.913390000 seconds]
  Frame Number: 4085
  Frame Length: 556 bytes (4448 bits)
  Capture Length: 556 bytes (4448 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 540
  Identification: 0x4ce0 (19680)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x3270 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 515, Ack: 173, Len: 488
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 515    (relative sequence number)
  [Next sequence number: 1003    (relative sequence number)]
  Acknowledgment number: 173    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 123
  [Calculated window size: 15744]
  [Window size scaling factor: 128]
  Checksum: 0xfbc1 [validation disabled]
    [Good Checksum: False]
```

```
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16455493, TSecr 54395547
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16455493
      Timestamp echo reply: 54395547
  [SEQ/ACK analysis]
    [Bytes in flight: 488]
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      [Message: GET /favicon.ico HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /favicon.ico
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Referer: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/838774620003efcb9c9d3a3ce2f4fe53\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/favicon.ico]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4088 125.933096000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 404 Not Found  (text
/html)

Frame 4088: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:10.964516000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340350.964516000 seconds
  [Time delta from previous captured frame: 0.000172000 seconds]
  [Time delta from previous displayed frame: 0.019706000 seconds]
  [Time since reference or first frame: 125.933096000 seconds]
  Frame Number: 4088
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x7d11 (32017)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x5102 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 536, Ack: 1003, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 536    (relative sequence number)
  [Next sequence number: 541    (relative sequence number)]
  Acknowledgment number: 1003    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 130
  [Calculated window size: 16640]
  [Window size scaling factor: 128]
```

```
  Checksum: 0x7d47 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54395597, TSecr 16455493
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54395597
      Timestamp echo reply: 16455493
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (368 bytes): #4086(363), #4088(5)]
  [Frame: 4086, payload: 0-362 (363 bytes)]
  [Frame: 4088, payload: 363-367 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 368]
Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      [Message: HTTP/1.1 404 Not Found\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 404
    Response Phrase: Not Found
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:07 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (196 octets)
      Chunk size: 196 octets
      Data (196 bytes)

0000  3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50   <!DOCTYPE HTML P
0010  55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f   UBLIC "-//IETF//
0020  44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e   DTD HTML 2.0//EN
0030  22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a   ">.<HTML><HEAD>.
0040  3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46   <TITLE>404 Not F
0050  6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48   ound</TITLE>.</H
0060  45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e   EAD><BODY>.<H1>N
0070  6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 50   ot Found</H1>.<P
0080  3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55   >The requested U
0090  52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64   RL was not found
00a0  20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e    on this server.
00b0  3c 2f 50 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54   </P>.</BODY></HT
00c0  4d 4c 3e 0a                                       ML>.
        Data: 3c21444f4354595045204854 4d4c205055424c494320222d...
        [Length: 196]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <HTML><HEAD>\n
  <TITLE>404 Not Found</TITLE>\n
```

```
</HEAD><BODY>\n
<H1>Not Found</H1>\n
<P>The requested URL was not found on this server.</P>\n
</BODY></HTML>\n
```

```
No.     Time           Source                Destination           Protocol Length Info
   4282 132.782252000  10.0.1.51             171.66.3.23           HTTP     221    GET /token?keywords=java&app_
id=9469ea8ba22b4786f382986111518038 HTTP/1.1

Frame 4282: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:17.813672000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340357.813672000 seconds
  [Time delta from previous captured frame: 0.006188000 seconds]
  [Time delta from previous displayed frame: 6.849156000 seconds]
  [Time since reference or first frame: 132.782252000 seconds]
  Frame Number: 4282
  Frame Length: 221 bytes (1768 bits)
  Capture Length: 221 bytes (1768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 205
  Identification: 0xfd32 (64818)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x836c [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60615 (60615), Dst Port: http (80), Seq: 1, Ack: 1, Len: 153
  Source port: 60615 (60615)
  Destination port: http (80)
  [Stream index: 171]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 154    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0xbd9e [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16457553, TSecr 54397648
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16457553
      Timestamp echo reply: 54397648
  [SEQ/ACK analysis]
    [Bytes in flight: 153]
Hypertext Transfer Protocol
  GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Message: GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: Keep-Alive\r\n
  User-Agent: adlib-android\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/token?keywords=java&app_id=9469ea8ba22b4786f382986111518038]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4286 132.796305000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 4286: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:17.827725000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340357.827725000 seconds
  [Time delta from previous captured frame: 0.000464000 seconds]
  [Time delta from previous displayed frame: 0.014053000 seconds]
  [Time since reference or first frame: 132.796305000 seconds]
  Frame Number: 4286
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xbb09 (47881)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x130a [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60615 (60615), Seq: 279, Ack: 154, Len: 5
  Source port: http (80)
  Destination port: 60615 (60615)
  [Stream index: 171]
  Sequence number: 279    (relative sequence number)
  [Next sequence number: 284    (relative sequence number)]
  Acknowledgment number: 154    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0x2d75 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54397658, TSecr 16457553
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54397658
      Timestamp echo reply: 16457553
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (283 bytes): #4284(278), #4286(5)]
  [Frame: 4284, payload: 0-277 (278 bytes)]
  [Frame: 4286, payload: 278-282 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 283]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:14 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (118 octets)
      Chunk size: 118 octets
      Data (118 bytes)

0000  3c 61 20 68 72 65 66 3d 22 2f 63 6c 69 63 6b 2f   <a href="/click/
0010  64 65 66 63 35 30 35 64 34 38 38 65 30 61 30 30   defc505d488e0a00
0020  66 66 39 32 66 37 62 30 61 63 31 63 33 38 63 37   ff92f7b0ac1c38c7
0030  2f 65 61 33 39 63 62 32 30 33 38 36 36 66 38 35   /ea39cb203866f85
0040  65 65 61 33 64 34 36 66 38 33 62 63 35 37 66 61   eea3d46f83bc57fa
0050  36 22 3e 43 6c 69 63 6b 20 68 65 72 65 20 74 6f   6">Click here to
0060  20 77 69 6e 20 24 31 30 30 2c 30 30 30 2c 30 30    win $100,000,00
0070  30 21 3c 2f 61 3e                                 0!</a>
      Data: 3c6120687265663d222f636c69636b2f6465666335303564...
      [Length: 118]
    Chunk boundary
  End of chunked encoding
    Chunk size: 0 octets
    Chunk boundary
Line-based text data: text/html
  <a href="/click/defc505d488e0a00ff92f7b0ac1c38c7/ea39cb203866f85eea3d46f83bc57fa6">Click here to win $100,000,00
  0!</a>
```

```
No.     Time           Source                Destination           Protocol Length Info
   4320 134.637099000  10.0.1.51             171.66.3.23           HTTP     582    GET /click/defc505d488e0a00ff
92f7b0ac1c38c7/ea39cb203866f85eea3d46f83bc57fa6 HTTP/1.1

Frame 4320: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:19.668519000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340359.668519000 seconds
  [Time delta from previous captured frame: 0.035329000 seconds]
  [Time delta from previous displayed frame: 1.840794000 seconds]
  [Time since reference or first frame: 134.637099000 seconds]
  Frame Number: 4320
  Frame Length: 582 bytes (4656 bits)
  Capture Length: 582 bytes (4656 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 566
  Identification: 0x4ce3 (19683)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x3253 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 1003, Ack: 541, Len: 514
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 1003    (relative sequence number)
  [Next sequence number: 1517    (relative sequence number)]
  Acknowledgment number: 541    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 131
  [Calculated window size: 16768]
  [Window size scaling factor: 128]
  Checksum: 0x11ef [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16458110, TSecr 54395597
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16458110
      Timestamp echo reply: 54395597
  [SEQ/ACK analysis]
    [Bytes in flight: 514]
Hypertext Transfer Protocol
  GET /click/defc505d488e0a00ff92f7b0ac1c38c7/ea39cb203866f85eea3d46f83bc57fa6 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /click/defc505d488e0a00ff92f7b0ac1c38c7/ea39cb203866f85eea3d46f83bc57fa6 HTTP/
    1.1\r\n]
      [Message: GET /click/defc505d488e0a00ff92f7b0ac1c38c7/ea39cb203866f85eea3d46f83bc57fa6 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /click/defc505d488e0a00ff92f7b0ac1c38c7/ea39cb203866f85eea3d46f83bc57fa6
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/ea39cb203866f85eea3d46f83bc57
  fa6]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4324 134.653663000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 4324: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:19.685083000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340359.685083000 seconds
  [Time delta from previous captured frame: 0.000209000 seconds]
  [Time delta from previous displayed frame: 0.016564000 seconds]
  [Time since reference or first frame: 134.653663000 seconds]
  Frame Number: 4324
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x9d2b (40235)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x30e8 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 708, Ack: 1517, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 708    (relative sequence number)
  [Next sequence number: 713    (relative sequence number)]
  Acknowledgment number: 1517    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 139
  [Calculated window size: 17792]
  [Window size scaling factor: 128]
  Checksum: 0x661d [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54398215, TSecr 16458110
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54398215
      Timestamp echo reply: 16458110
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (172 bytes): #4322(167), #4324(5)]
  [Frame: 4322, payload: 0-166 (167 bytes)]
  [Frame: 4324, payload: 167-171 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 172]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:15 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (8 octets)
      Chunk size: 8 octets
      Data (8 bytes)

0000  53 75 63 63 65 73 73 21                           Success!
        Data: 5375636365737321
        [Length: 8]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  Success!
```

```
No.     Time           Source                Destination           Protocol Length Info
   4331 134.720777000  10.0.1.51             171.66.3.23           HTTP     556    GET /favicon.ico HTTP/1.1

Frame 4331: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:19.752197000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340359.752197000 seconds
  [Time delta from previous captured frame: 0.018537000 seconds]
  [Time delta from previous displayed frame: 0.067114000 seconds]
  [Time since reference or first frame: 134.720777000 seconds]
  Frame Number: 4331
  Frame Length: 556 bytes (4448 bits)
  Capture Length: 556 bytes (4448 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 540
  Identification: 0x4ce6 (19686)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x326a [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 1517, Ack: 713, Len: 488
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 1517    (relative sequence number)
  [Next sequence number: 2005    (relative sequence number)]
  Acknowledgment number: 713    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 140
  [Calculated window size: 17920]
  [Window size scaling factor: 128]
  Checksum: 0xc79e [validation disabled]
    [Good Checksum: False]
```

```
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16458135, TSecr 54398215
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16458135
      Timestamp echo reply: 54398215
  [SEQ/ACK analysis]
    [Bytes in flight: 488]
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      [Message: GET /favicon.ico HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /favicon.ico
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Referer: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/ea39cb203866f85eea3d46f83bc57fa6\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/favicon.ico]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4334 134.739080000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 404 Not Found  (text
/html)

Frame 4334: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:19.770500000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340359.770500000 seconds
  [Time delta from previous captured frame: 0.000814000 seconds]
  [Time delta from previous displayed frame: 0.018303000 seconds]
  [Time since reference or first frame: 134.739080000 seconds]
  Frame Number: 4334
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x306b (12395)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x9da8 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 1076, Ack: 2005, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 1076    (relative sequence number)
  [Next sequence number: 1081    (relative sequence number)]
  Acknowledgment number: 2005    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 147
  [Calculated window size: 18816]
  [Window size scaling factor: 128]
```

```
  Checksum: 0x628b [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54398240, TSecr 16458135
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54398240
      Timestamp echo reply: 16458135
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (368 bytes): #4332(363), #4334(5)]
  [Frame: 4332, payload: 0-362 (363 bytes)]
  [Frame: 4334, payload: 363-367 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 368]
Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      [Message: HTTP/1.1 404 Not Found\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 404
    Response Phrase: Not Found
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:15 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (196 octets)
      Chunk size: 196 octets
      Data (196 bytes)

0000  3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50   <!DOCTYPE HTML P
0010  55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f   UBLIC "-//IETF//
0020  44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e   DTD HTML 2.0//EN
0030  22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a   ">.<HTML><HEAD>.
0040  3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46   <TITLE>404 Not F
0050  6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48   ound</TITLE>.</H
0060  45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e   EAD><BODY>.<H1>N
0070  6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 50   ot Found</H1>.<P
0080  3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55   >The requested U
0090  52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64   RL was not found
00a0  20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e    on this server.
00b0  3c 2f 50 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54   </P>.</BODY></HT
00c0  4d 4c 3e 0a                                       ML>.
        Data: 3c21444f4354595045204854 4d4c205055424c494320222d...
        [Length: 196]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <HTML><HEAD>\n
  <TITLE>404 Not Found</TITLE>\n
```

```
</HEAD><BODY>\n
<H1>Not Found</H1>\n
<P>The requested URL was not found on this server.</P>\n
</BODY></HTML>\n
```

```
No.     Time           Source                Destination           Protocol Length Info
   4439 140.996644000  10.0.1.51             171.66.3.23           HTTP     221    GET /token?keywords=java&app_
id=9469ea8ba22b4786f382986111518038 HTTP/1.1

Frame 4439: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:26.028064000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340366.028064000 seconds
  [Time delta from previous captured frame: 0.047627000 seconds]
  [Time delta from previous displayed frame: 6.257564000 seconds]
  [Time since reference or first frame: 140.996644000 seconds]
  Frame Number: 4439
  Frame Length: 221 bytes (1768 bits)
  Capture Length: 221 bytes (1768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 205
  Identification: 0xb225 (45605)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0xce79 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60618 (60618), Dst Port: http (80), Seq: 1, Ack: 1, Len: 153
  Source port: 60618 (60618)
  Destination port: http (80)
  [Stream index: 174]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 154    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0x3c75 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16460018, TSecr 54400083
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16460018
      Timestamp echo reply: 54400083
  [SEQ/ACK analysis]
    [Bytes in flight: 153]
Hypertext Transfer Protocol
  GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Message: GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: Keep-Alive\r\n
  User-Agent: adlib-android\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/token?keywords=java&app_id=9469ea8ba22b4786f382986111518038]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4443 141.013882000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 4443: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:26.045302000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340366.045302000 seconds
  [Time delta from previous captured frame: 0.001541000 seconds]
  [Time delta from previous displayed frame: 0.017238000 seconds]
  [Time since reference or first frame: 141.013882000 seconds]
  Frame Number: 4443
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x3946 (14662)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x94cd [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60618 (60618), Seq: 279, Ack: 154, Len: 5
  Source port: http (80)
  Destination port: 60618 (60618)
  [Stream index: 174]
  Sequence number: 279    (relative sequence number)
  [Next sequence number: 284    (relative sequence number)]
  Acknowledgment number: 154    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0xac2e [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54400122, TSecr 16460018
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54400122
      Timestamp echo reply: 16460018
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (283 bytes): #4441(278), #4443(5)]
  [Frame: 4441, payload: 0-277 (278 bytes)]
  [Frame: 4443, payload: 278-282 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 283]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:22 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (118 octets)
      Chunk size: 118 octets
      Data (118 bytes)

0000  3c 61 20 68 72 65 66 3d 22 2f 63 6c 69 63 6b 2f   <a href="/click/
0010  64 65 66 63 35 30 35 64 34 38 38 65 30 61 30 30   defc505d488e0a00
0020  66 66 39 32 66 37 62 30 61 63 31 63 33 38 63 37   ff92f7b0ac1c38c7
0030  2f 32 62 34 62 66 62 38 31 64 32 38 36 38 38 32   /2b4bfb81d286882
0040  33 31 38 37 33 61 37 33 38 65 39 36 38 36 65 37   31873a738e9686e7
0050  33 22 3e 43 6c 69 63 6b 20 68 65 72 65 20 74 6f   3">Click here to
0060  20 77 69 6e 20 24 31 30 30 2c 30 30 30 2c 30 30    win $100,000,00
0070  30 21 3c 2f 61 3e                                 0!</a>
      Data: 3c6120687265663d222f636c69636b2f6465666335303564...
      [Length: 118]
    Chunk boundary
  End of chunked encoding
    Chunk size: 0 octets
    Chunk boundary
Line-based text data: text/html
  <a href="/click/defc505d488e0a00ff92f7b0ac1c38c7/2b4bfb81d28688231873a738e9686e73">Click here to win $100,000,00
  0!</a>
```

```
No.     Time           Source                Destination           Protocol Length Info
   4501 150.043147000  10.0.1.51             171.66.3.23           HTTP     221    GET /token?keywords=java&app_
id=9469ea8ba22b4786f382986111518038 HTTP/1.1

Frame 4501: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:35.074567000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340375.074567000 seconds
  [Time delta from previous captured frame: 0.001817000 seconds]
  [Time delta from previous displayed frame: 9.029265000 seconds]
  [Time since reference or first frame: 150.043147000 seconds]
  Frame Number: 4501
  Frame Length: 221 bytes (1768 bits)
  Capture Length: 221 bytes (1768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 205
  Identification: 0x6537 (25911)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x1b68 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60622 (60622), Dst Port: http (80), Seq: 1, Ack: 1, Len: 153
  Source port: 60622 (60622)
  Destination port: http (80)
  [Stream index: 178]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 154    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0xcac2 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16462732, TSecr 54402828
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16462732
      Timestamp echo reply: 54402828
  [SEQ/ACK analysis]
    [Bytes in flight: 153]
Hypertext Transfer Protocol
  GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Message: GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: Keep-Alive\r\n
  User-Agent: adlib-android\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/token?keywords=java&app_id=9469ea8ba22b4786f382986111518038]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4515 150.107823000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 4515: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:35.139243000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340375.139243000 seconds
  [Time delta from previous captured frame: 0.001594000 seconds]
  [Time delta from previous displayed frame: 0.064676000 seconds]
  [Time since reference or first frame: 150.107823000 seconds]
  Frame Number: 4515
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xb858 (47192)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x15bb [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60622 (60622), Seq: 279, Ack: 154, Len: 5
  Source port: http (80)
  Destination port: 60622 (60622)
  [Stream index: 178]
  Sequence number: 279    (relative sequence number)
  [Next sequence number: 284    (relative sequence number)]
  Acknowledgment number: 154    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0x3a9b [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54402836, TSecr 16462732
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54402836
      Timestamp echo reply: 16462732
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (283 bytes): #4513(278), #4515(5)]
  [Frame: 4513, payload: 0-277 (278 bytes)]
  [Frame: 4515, payload: 278-282 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 283]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:31 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (118 octets)
      Chunk size: 118 octets
      Data (118 bytes)

0000  3c 61 20 68 72 65 66 3d 22 2f 63 6c 69 63 6b 2f   <a href="/click/
0010  64 65 66 63 35 30 35 64 34 38 38 65 30 61 30 30   defc505d488e0a00
0020  66 66 39 32 66 37 62 30 61 63 31 63 33 38 63 37   ff92f7b0ac1c38c7
0030  2f 63 63 33 62 32 63 39 62 32 39 37 61 66 33 62   /cc3b2c9b297af3b
0040  39 33 30 61 32 65 39 37 37 31 33 37 38 38 32 38   930a2e9771378828
0050  35 22 3e 43 6c 69 63 6b 20 68 65 72 65 20 74 6f   5">Click here to
0060  20 77 69 6e 20 24 31 30 30 2c 30 30 30 2c 30 30    win $100,000,00
0070  30 21 3c 2f 61 3e                                 0!</a>
      Data: 3c6120687265663d222f636c69636b2f6465666335303564...
      [Length: 118]
    Chunk boundary
  End of chunked encoding
    Chunk size: 0 octets
    Chunk boundary
Line-based text data: text/html
  <a href="/click/defc505d488e0a00ff92f7b0ac1c38c7/cc3b2c9b297af3b930a2e97713788285">Click here to win $100,000,00
  0!</a>
```

```
No.     Time           Source                Destination           Protocol Length Info
   4561 152.313501000  10.0.1.51             171.66.3.23           HTTP     582    GET /click/defc505d488e0a00ff
92f7b0ac1c38c7/cc3b2c9b297af3b930a2e97713788285 HTTP/1.1

Frame 4561: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:37.344921000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340377.344921000 seconds
  [Time delta from previous captured frame: 0.001150000 seconds]
  [Time delta from previous displayed frame: 2.205678000 seconds]
  [Time since reference or first frame: 152.313501000 seconds]
  Frame Number: 4561
  Frame Length: 582 bytes (4656 bits)
  Capture Length: 582 bytes (4656 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 566
  Identification: 0x4ce9 (19689)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x324d [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 2005, Ack: 1081, Len: 514
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 2005    (relative sequence number)
  [Next sequence number: 2519    (relative sequence number)]
  Acknowledgment number: 1081    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 148
  [Calculated window size: 18944]
  [Window size scaling factor: 128]
  Checksum: 0x4437 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16463413, TSecr 54398240
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16463413
      Timestamp echo reply: 54398240
  [SEQ/ACK analysis]
    [Bytes in flight: 514]
Hypertext Transfer Protocol
  GET /click/defc505d488e0a00ff92f7b0ac1c38c7/cc3b2c9b297af3b930a2e97713788285 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /click/defc505d488e0a00ff92f7b0ac1c38c7/cc3b2c9b297af3b930a2e97713788285 HTTP/
    1.1\r\n]
      [Message: GET /click/defc505d488e0a00ff92f7b0ac1c38c7/cc3b2c9b297af3b930a2e97713788285 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /click/defc505d488e0a00ff92f7b0ac1c38c7/cc3b2c9b297af3b930a2e97713788285
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/cc3b2c9b297af3b930a2e97713788
  285]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4564 152.332061000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 4564: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:37.363481000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340377.363481000 seconds
  [Time delta from previous captured frame: 0.000518000 seconds]
  [Time delta from previous displayed frame: 0.018560000 seconds]
  [Time since reference or first frame: 152.332061000 seconds]
  Frame Number: 4564
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xea5a (59994)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0xe3b8 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 1248, Ack: 2519, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 1248    (relative sequence number)
  [Next sequence number: 1253    (relative sequence number)]
  Acknowledgment number: 2519    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 155
  [Calculated window size: 19840]
  [Window size scaling factor: 128]
  Checksum: 0x369a [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54403517, TSecr 16463413
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54403517
      Timestamp echo reply: 16463413
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (172 bytes): #4562(167), #4564(5)]
  [Frame: 4562, payload: 0-166 (167 bytes)]
  [Frame: 4564, payload: 167-171 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 172]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:33 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (8 octets)
      Chunk size: 8 octets
      Data (8 bytes)

0000  53 75 63 63 65 73 73 21                           Success!
        Data: 5375636365737321
        [Length: 8]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  Success!
```

```
No.     Time           Source                Destination           Protocol Length Info
   4570 152.376576000  10.0.1.51             171.66.3.23           HTTP     556    GET /favicon.ico HTTP/1.1

Frame 4570: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:37.407996000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340377.407996000 seconds
  [Time delta from previous captured frame: 0.009740000 seconds]
  [Time delta from previous displayed frame: 0.044515000 seconds]
  [Time since reference or first frame: 152.376576000 seconds]
  Frame Number: 4570
  Frame Length: 556 bytes (4448 bits)
  Capture Length: 556 bytes (4448 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 540
  Identification: 0x4cec (19692)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x3264 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 2519, Ack: 1253, Len: 488
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 2519    (relative sequence number)
  [Next sequence number: 3007    (relative sequence number)]
  Acknowledgment number: 1253    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 156
  [Calculated window size: 19968]
  [Window size scaling factor: 128]
  Checksum: 0x0179 [validation disabled]
    [Good Checksum: False]
```

```
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16463432, TSecr 54403517
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16463432
      Timestamp echo reply: 54403517
  [SEQ/ACK analysis]
    [Bytes in flight: 488]
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      [Message: GET /favicon.ico HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /favicon.ico
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Referer: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/cc3b2c9b297af3b930a2e97713788285\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/favicon.ico]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4574 152.393219000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 404 Not Found  (text
/html)

Frame 4574: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:37.424639000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340377.424639000 seconds
  [Time delta from previous captured frame: 0.000268000 seconds]
  [Time delta from previous displayed frame: 0.016643000 seconds]
  [Time since reference or first frame: 152.393219000 seconds]
  Frame Number: 4574
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x4331 (17201)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x8ae2 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 1616, Ack: 3007, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 1616    (relative sequence number)
  [Next sequence number: 1621    (relative sequence number)]
  Acknowledgment number: 3007    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 164
  [Calculated window size: 20992]
  [Window size scaling factor: 128]
```

```
  Checksum: 0x3312 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54403537, TSecr 16463432
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54403537
      Timestamp echo reply: 16463432
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (368 bytes): #4572(363), #4574(5)]
  [Frame: 4572, payload: 0-362 (363 bytes)]
  [Frame: 4574, payload: 363-367 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 368]
Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      [Message: HTTP/1.1 404 Not Found\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 404
    Response Phrase: Not Found
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:33 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (196 octets)
      Chunk size: 196 octets
      Data (196 bytes)

0000  3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50   <!DOCTYPE HTML P
0010  55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f   UBLIC "-//IETF//
0020  44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e   DTD HTML 2.0//EN
0030  22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a   ">.<HTML><HEAD>.
0040  3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46   <TITLE>404 Not F
0050  6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48   ound</TITLE>.</H
0060  45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e   EAD><BODY>.<H1>N
0070  6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 50   ot Found</H1>.<P
0080  3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55   >The requested U
0090  52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64   RL was not found
00a0  20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e    on this server.
00b0  3c 2f 50 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54   </P>.</BODY></HT
00c0  4d 4c 3e 0a                                       ML>.
        Data: 3c21444f4354595045204854544d4c205055424c494320222d...
        [Length: 196]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <HTML><HEAD>\n
  <TITLE>404 Not Found</TITLE>\n
```

```
</HEAD><BODY>\n
<H1>Not Found</H1>\n
<P>The requested URL was not found on this server.</P>\n
</BODY></HTML>\n
```

```
No.     Time           Source                Destination           Protocol Length Info
   4683 164.191895000  10.0.1.51             171.66.3.23           HTTP     221    GET /token?keywords=java&app_
id=9469ea8ba22b4786f382986111518038 HTTP/1.1

Frame 4683: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:49.223315000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340389.223315000 seconds
  [Time delta from previous captured frame: 0.019543000 seconds]
  [Time delta from previous displayed frame: 11.798676000 seconds]
  [Time since reference or first frame: 164.191895000 seconds]
  Frame Number: 4683
  Frame Length: 221 bytes (1768 bits)
  Capture Length: 221 bytes (1768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 205
  Identification: 0x8821 (34849)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0xf87d [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60628 (60628), Dst Port: http (80), Seq: 1, Ack: 1, Len: 153
  Source port: 60628 (60628)
  Destination port: http (80)
  [Stream index: 184]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 154    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0xf319 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16466976, TSecr 54407070
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16466976
      Timestamp echo reply: 54407070
  [SEQ/ACK analysis]
    [Bytes in flight: 153]
Hypertext Transfer Protocol
  GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Message: GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: Keep-Alive\r\n
  User-Agent: adlib-android\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/token?keywords=java&app_id=9469ea8ba22b4786f382986111518038]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4687 164.214142000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 4687: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:49.245562000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340389.245562000 seconds
  [Time delta from previous captured frame: 0.000441000 seconds]
  [Time delta from previous displayed frame: 0.022247000 seconds]
  [Time since reference or first frame: 164.214142000 seconds]
  Frame Number: 4687
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x6d29 (27945)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x60ea [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60628 (60628), Seq: 279, Ack: 154, Len: 5
  Source port: http (80)
  Destination port: 60628 (60628)
  [Stream index: 184]
  Sequence number: 279    (relative sequence number)
  [Next sequence number: 284    (relative sequence number)]
  Acknowledgment number: 154    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0x62f0 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54407080, TSecr 16466976
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54407080
      Timestamp echo reply: 16466976
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (283 bytes): #4685(278), #4687(5)]
  [Frame: 4685, payload: 0-277 (278 bytes)]
  [Frame: 4687, payload: 278-282 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 283]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:45 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (118 octets)
      Chunk size: 118 octets
      Data (118 bytes)

0000  3c 61 20 68 72 65 66 3d 22 2f 63 6c 69 63 6b 2f   <a href="/click/
0010  64 65 66 63 35 30 35 64 34 38 38 65 30 61 30 30   defc505d488e0a00
0020  66 66 39 32 66 37 62 30 61 63 31 63 33 38 63 37   ff92f7b0ac1c38c7
0030  2f 65 65 64 30 62 66 31 63 62 31 66 64 38 36 34   /eed0bf1cb1fd864
0040  32 39 36 35 34 32 33 64 65 30 31 30 34 33 30 34   2965423de0104304
0050  64 22 3e 43 6c 69 63 6b 20 68 65 72 65 20 74 6f   d">Click here to
0060  20 77 69 6e 20 24 31 30 30 2c 30 30 30 2c 30 30    win $100,000,00
0070  30 21 3c 2f 61 3e                                 0!</a>
        Data: 3c6120687265663d222f636c69636b2f6465666335303564...
        [Length: 118]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <a href="/click/defc505d488e0a00ff92f7b0ac1c38c7/eed0bf1cb1fd8642965423de0104304d">Click here to win $100,000,00
  0!</a>
```

```
No.     Time           Source                Destination           Protocol Length Info
   4734 166.416279000  10.0.1.51             171.66.3.23           HTTP     582    GET /click/defc505d488e0a00ff
92f7b0ac1c38c7/eed0bf1cb1fd8642965423de0104304d HTTP/1.1

Frame 4734: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:51.447699000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340391.447699000 seconds
  [Time delta from previous captured frame: 0.007260000 seconds]
  [Time delta from previous displayed frame: 2.202137000 seconds]
  [Time since reference or first frame: 166.416279000 seconds]
  Frame Number: 4734
  Frame Length: 582 bytes (4656 bits)
  Capture Length: 582 bytes (4656 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 566
  Identification: 0x4cef (19695)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x3247 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 3007, Ack: 1621, Len: 514
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 3007    (relative sequence number)
  [Next sequence number: 3521    (relative sequence number)]
  Acknowledgment number: 1621    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 165
  [Calculated window size: 21120]
  [Window size scaling factor: 128]
  Checksum: 0xf7c5 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16467644, TSecr 54403537
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16467644
      Timestamp echo reply: 54403537
  [SEQ/ACK analysis]
    [Bytes in flight: 514]
Hypertext Transfer Protocol
  GET /click/defc505d488e0a00ff92f7b0ac1c38c7/eed0bf1cb1fd8642965423de0104304d HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /click/defc505d488e0a00ff92f7b0ac1c38c7/eed0bf1cb1fd8642965423de0104304d HTTP/
    1.1\r\n]
      [Message: GET /click/defc505d488e0a00ff92f7b0ac1c38c7/eed0bf1cb1fd8642965423de0104304d HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /click/defc505d488e0a00ff92f7b0ac1c38c7/eed0bf1cb1fd8642965423de0104304d
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/eed0bf1cb1fd8642965423de01043
  04d]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4741 166.430510000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 4741: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:51.461930000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340391.461930000 seconds
  [Time delta from previous captured frame: 0.000439000 seconds]
  [Time delta from previous displayed frame: 0.014231000 seconds]
  [Time since reference or first frame: 166.430510000 seconds]
  Frame Number: 4741
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x8f7c (36732)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x3e97 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 1788, Ack: 3521, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 1788    (relative sequence number)
  [Next sequence number: 1793    (relative sequence number)]
  Acknowledgment number: 3521    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 172
  [Calculated window size: 22016]
  [Window size scaling factor: 128]
  Checksum: 0x0f75 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54407748, TSecr 16467644
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54407748
      Timestamp echo reply: 16467644
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (172 bytes): #4739(167), #4741(5)]
  [Frame: 4739, payload: 0-166 (167 bytes)]
  [Frame: 4741, payload: 167-171 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 172]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:47 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (8 octets)
      Chunk size: 8 octets
      Data (8 bytes)

0000  53 75 63 63 65 73 73 21                           Success!
        Data: 5375636365737321
        [Length: 8]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  Success!
```

```
No.     Time           Source                Destination           Protocol Length Info
   4744 166.466723000  10.0.1.51             171.66.3.23           HTTP     556    GET /favicon.ico HTTP/1.1

Frame 4744: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:51.498143000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340391.498143000 seconds
  [Time delta from previous captured frame: 0.026226000 seconds]
  [Time delta from previous displayed frame: 0.036213000 seconds]
  [Time since reference or first frame: 166.466723000 seconds]
  Frame Number: 4744
  Frame Length: 556 bytes (4448 bits)
  Capture Length: 556 bytes (4448 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 540
  Identification: 0x4cf2 (19698)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x325e [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 3521, Ack: 1793, Len: 488
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 3521    (relative sequence number)
  [Next sequence number: 4009    (relative sequence number)]
  Acknowledgment number: 1793    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 173
  [Calculated window size: 22144]
  [Window size scaling factor: 128]
  Checksum: 0xb836 [validation disabled]
    [Good Checksum: False]
```

```
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16467659, TSecr 54407748
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16467659
      Timestamp echo reply: 54407748
  [SEQ/ACK analysis]
    [Bytes in flight: 488]
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      [Message: GET /favicon.ico HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /favicon.ico
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Referer: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/eed0bf1cb1fd8642965423de0104304d\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/favicon.ico]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4746 166.497925000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 404 Not Found  (text
/html)

Frame 4746: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:51.529345000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340391.529345000 seconds
  [Time delta from previous captured frame: 0.000455000 seconds]
  [Time delta from previous displayed frame: 0.031202000 seconds]
  [Time since reference or first frame: 166.497925000 seconds]
  Frame Number: 4746
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xa459 (42073)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x29ba [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 2156, Ack: 4009, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 2156    (relative sequence number)
  [Next sequence number: 2161    (relative sequence number)]
  Acknowledgment number: 4009    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 181
  [Calculated window size: 23168]
  [Window size scaling factor: 128]
```

```
  Checksum: 0x0bf1 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54407768, TSecr 16467659
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54407768
      Timestamp echo reply: 16467659
  [SEQ/ACK analysis]
    [Bytes in flight: 368]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (368 bytes): #4745(363), #4746(5)]
  [Frame: 4745, payload: 0-362 (363 bytes)]
  [Frame: 4746, payload: 363-367 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 368]
Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      [Message: HTTP/1.1 404 Not Found\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 404
    Response Phrase: Not Found
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:47 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (196 octets)
      Chunk size: 196 octets
      Data (196 bytes)

0000  3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50   <!DOCTYPE HTML P
0010  55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f   UBLIC "-//IETF//
0020  44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e   DTD HTML 2.0//EN
0030  22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a   ">.<HTML><HEAD>.
0040  3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46   <TITLE>404 Not F
0050  6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48   ound</TITLE>.</H
0060  45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e   EAD><BODY>.<H1>N
0070  6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 50   ot Found</H1>.<P
0080  3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55   >The requested U
0090  52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64   RL was not found
00a0  20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e    on this server.
00b0  3c 2f 50 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54   </P>.</BODY></HT
00c0  4d 4c 3e 0a                                       ML>.
        Data: 3c21444f4354595045204854544d4c205055424c494320222d...
        [Length: 196]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <HTML><HEAD>\n
  <TITLE>404 Not Found</TITLE>\n
```

```
</HEAD><BODY>\n
<H1>Not Found</H1>\n
<P>The requested URL was not found on this server.</P>\n
</BODY></HTML>\n
```

```
No.     Time           Source                Destination           Protocol Length Info
   4839 172.963984000  10.0.1.51             171.66.3.23           HTTP     221    GET /token?keywords=java&app_
id=9469ea8ba22b4786f382986111518038 HTTP/1.1

Frame 4839: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:57.995404000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340397.995404000 seconds
  [Time delta from previous captured frame: 0.009007000 seconds]
  [Time delta from previous displayed frame: 6.466059000 seconds]
  [Time since reference or first frame: 172.963984000 seconds]
  Frame Number: 4839
  Frame Length: 221 bytes (1768 bits)
  Capture Length: 221 bytes (1768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 205
  Identification: 0x459b (17819)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x3b04 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60632 (60632), Dst Port: http (80), Seq: 1, Ack: 1, Len: 153
  Source port: 60632 (60632)
  Destination port: http (80)
  [Stream index: 188]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 154    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0x7f5a [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16469608, TSecr 54409705
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16469608
      Timestamp echo reply: 54409705
  [SEQ/ACK analysis]
    [Bytes in flight: 153]
Hypertext Transfer Protocol
  GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Message: GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: Keep-Alive\r\n
  User-Agent: adlib-android\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/token?keywords=java&app_id=9469ea8ba22b4786f382986111518038]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4843 172.977816000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 4843: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:19:58.009236000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340398.009236000 seconds
  [Time delta from previous captured frame: 0.000472000 seconds]
  [Time delta from previous displayed frame: 0.013832000 seconds]
  [Time since reference or first frame: 172.977816000 seconds]
  Frame Number: 4843
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xa215 (41493)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x2bfe [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60632 (60632), Seq: 279, Ack: 154, Len: 5
  Source port: http (80)
  Destination port: 60632 (60632)
  [Stream index: 188]
  Sequence number: 279    (relative sequence number)
  [Next sequence number: 284    (relative sequence number)]
  Acknowledgment number: 154    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0xef33 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54409712, TSecr 16469608
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54409712
      Timestamp echo reply: 16469608
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (283 bytes): #4841(278), #4843(5)]
  [Frame: 4841, payload: 0-277 (278 bytes)]
  [Frame: 4843, payload: 278-282 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 283]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:54 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (118 octets)
      Chunk size: 118 octets
      Data (118 bytes)

0000  3c 61 20 68 72 65 66 3d 22 2f 63 6c 69 63 6b 2f   <a href="/click/
0010  64 65 66 63 35 30 35 64 34 38 38 65 30 61 30 30   defc505d488e0a00
0020  66 66 39 32 66 37 62 30 61 63 31 63 33 38 63 37   ff92f7b0ac1c38c7
0030  2f 36 37 31 63 36 63 63 36 36 62 61 65 62 36 63   /671c6cc66baeb6c
0040  33 38 31 35 62 32 66 62 34 36 61 64 34 65 31 33   3815b2fb46ad4e13
0050  31 22 3e 43 6c 69 63 6b 20 68 65 72 65 20 74 6f   1">Click here to
0060  20 77 69 6e 20 24 31 30 30 2c 30 30 30 2c 30 30    win $100,000,00
0070  30 21 3c 2f 61 3e                                 0!</a>
      Data: 3c6120687265663d222f636c69636b2f6465666335303564...
      [Length: 118]
    Chunk boundary
  End of chunked encoding
    Chunk size: 0 octets
    Chunk boundary
Line-based text data: text/html
  <a href="/click/defc505d488e0a00ff92f7b0ac1c38c7/671c6cc66baeb6c3815b2fb46ad4e131">Click here to win $100,000,00
  0!</a>
```

```
No.     Time           Source                Destination           Protocol Length Info
   4894 175.083112000  10.0.1.51             171.66.3.23           HTTP     582    GET /click/defc505d488e0a00ff
92f7b0ac1c38c7/671c6cc66baeb6c3815b2fb46ad4e131 HTTP/1.1

Frame 4894: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:00.114532000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340400.114532000 seconds
  [Time delta from previous captured frame: 0.051423000 seconds]
  [Time delta from previous displayed frame: 2.105296000 seconds]
  [Time since reference or first frame: 175.083112000 seconds]
  Frame Number: 4894
  Frame Length: 582 bytes (4656 bits)
  Capture Length: 582 bytes (4656 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 566
  Identification: 0x4cf4 (19700)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x3242 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 4009, Ack: 2161, Len: 514
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 4009    (relative sequence number)
  [Next sequence number: 4523    (relative sequence number)]
  Acknowledgment number: 2161    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 182
  [Calculated window size: 23296]
  [Window size scaling factor: 128]
  Checksum: 0xa2ce [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16470244, TSecr 54407768
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16470244
      Timestamp echo reply: 54407768
  [SEQ/ACK analysis]
    [Bytes in flight: 514]
Hypertext Transfer Protocol
  GET /click/defc505d488e0a00ff92f7b0ac1c38c7/671c6cc66baeb6c3815b2fb46ad4e131 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /click/defc505d488e0a00ff92f7b0ac1c38c7/671c6cc66baeb6c3815b2fb46ad4e131 HTTP/
    1.1\r\n]
      [Message: GET /click/defc505d488e0a00ff92f7b0ac1c38c7/671c6cc66baeb6c3815b2fb46ad4e131 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /click/defc505d488e0a00ff92f7b0ac1c38c7/671c6cc66baeb6c3815b2fb46ad4e131
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/671c6cc66baeb6c3815b2fb46ad4e
  131]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4896 175.099642000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 4896: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:00.131062000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340400.131062000 seconds
  [Time delta from previous captured frame: 0.000448000 seconds]
  [Time delta from previous displayed frame: 0.016530000 seconds]
  [Time since reference or first frame: 175.099642000 seconds]
  Frame Number: 4896
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x8b12 (35602)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x4301 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 2328, Ack: 4523, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 2328    (relative sequence number)
  [Next sequence number: 2333    (relative sequence number)]
  Acknowledgment number: 4523    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 189
  [Calculated window size: 24192]
  [Window size scaling factor: 128]
  Checksum: 0xf50d [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54410348, TSecr 16470244
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54410348
      Timestamp echo reply: 16470244
  [SEQ/ACK analysis]
    [Bytes in flight: 172]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (172 bytes): #4895(167), #4896(5)]
  [Frame: 4895, payload: 0-166 (167 bytes)]
  [Frame: 4896, payload: 167-171 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 172]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:56 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (8 octets)
      Chunk size: 8 octets
      Data (8 bytes)

0000  53 75 63 63 65 73 73 21                           Success!
        Data: 5375636365737321
        [Length: 8]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  Success!
```

```
No.     Time           Source                Destination           Protocol Length Info
   4903 175.138724000  10.0.1.51             171.66.3.23           HTTP     556    GET /favicon.ico HTTP/1.1

Frame 4903: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:00.170144000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340400.170144000 seconds
  [Time delta from previous captured frame: 0.006457000 seconds]
  [Time delta from previous displayed frame: 0.039082000 seconds]
  [Time since reference or first frame: 175.138724000 seconds]
  Frame Number: 4903
  Frame Length: 556 bytes (4448 bits)
  Capture Length: 556 bytes (4448 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 540
  Identification: 0x4cf6 (19702)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x325a [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 4523, Ack: 2333, Len: 488
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 4523    (relative sequence number)
  [Next sequence number: 5011    (relative sequence number)]
  Acknowledgment number: 2333    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 190
  [Calculated window size: 24320]
  [Window size scaling factor: 128]
  Checksum: 0x6c9a [validation disabled]
    [Good Checksum: False]
```

```
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16470260, TSecr 54410348
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16470260
      Timestamp echo reply: 54410348
  [SEQ/ACK analysis]
    [Bytes in flight: 488]
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      [Message: GET /favicon.ico HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /favicon.ico
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Referer: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/671c6cc66baeb6c3815b2fb46ad4e131\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/favicon.ico]
```

```
No.     Time           Source                Destination           Protocol Length Info
   4905 175.155146000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 404 Not Found  (text
/html)

Frame 4905: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:00.186566000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340400.186566000 seconds
  [Time delta from previous captured frame: 0.000236000 seconds]
  [Time delta from previous displayed frame: 0.016422000 seconds]
  [Time since reference or first frame: 175.155146000 seconds]
  Frame Number: 4905
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x3e6f (15983)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x8fa4 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 2696, Ack: 5011, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 2696    (relative sequence number)
  [Next sequence number: 2701    (relative sequence number)]
  Acknowledgment number: 5011    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 197
  [Calculated window size: 25216]
  [Window size scaling factor: 128]
```

```
  Checksum: 0xf18c [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54410365, TSecr 16470260
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54410365
      Timestamp echo reply: 16470260
  [SEQ/ACK analysis]
    [Bytes in flight: 368]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (368 bytes): #4904(363), #4905(5)]
  [Frame: 4904, payload: 0-362 (363 bytes)]
  [Frame: 4905, payload: 363-367 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 368]
Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      [Message: HTTP/1.1 404 Not Found\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 404
    Response Phrase: Not Found
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:20:56 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (196 octets)
      Chunk size: 196 octets
      Data (196 bytes)

0000  3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50   <!DOCTYPE HTML P
0010  55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f   UBLIC "-//IETF//
0020  44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e   DTD HTML 2.0//EN
0030  22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a   ">.<HTML><HEAD>.
0040  3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46   <TITLE>404 Not F
0050  6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48   ound</TITLE>.</H
0060  45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e   EAD><BODY>.<H1>N
0070  6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 50   ot Found</H1>.<P
0080  3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55   >The requested U
0090  52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64   RL was not found
00a0  20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e    on this server.
00b0  3c 2f 50 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54   </P>.</BODY></HT
00c0  4d 4c 3e 0a                                       ML>.
        Data: 3c21444f4354595045204854 4d4c205055424c494320222d...
        [Length: 196]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <HTML><HEAD>\n
  <TITLE>404 Not Found</TITLE>\n
```

```
</HEAD><BODY>\n
<H1>Not Found</H1>\n
<P>The requested URL was not found on this server.</P>\n
</BODY></HTML>\n
```

```
No.     Time           Source                Destination           Protocol Length Info
   5161 185.262186000  10.0.1.51             171.66.3.23           HTTP     221    GET /token?keywords=java&app_
id=9469ea8ba22b4786f382986111518038 HTTP/1.1

Frame 5161: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:10.293606000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340410.293606000 seconds
  [Time delta from previous captured frame: 0.049833000 seconds]
  [Time delta from previous displayed frame: 10.107040000 seconds]
  [Time since reference or first frame: 185.262186000 seconds]
  Frame Number: 5161
  Frame Length: 221 bytes (1768 bits)
  Capture Length: 221 bytes (1768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 205
  Identification: 0xc48a (50314)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0xbc14 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60637 (60637), Dst Port: http (80), Seq: 1, Ack: 1, Len: 153
  Source port: 60637 (60637)
  Destination port: http (80)
  [Stream index: 193]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 154    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0xbcfa [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16473297, TSecr 54413370
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16473297
      Timestamp echo reply: 54413370
  [SEQ/ACK analysis]
    [Bytes in flight: 153]
Hypertext Transfer Protocol
  GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Message: GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: Keep-Alive\r\n
  User-Agent: adlib-android\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/token?keywords=java&app_id=9469ea8ba22b4786f382986111518038]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5165 185.280308000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 5165: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:10.311728000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340410.311728000 seconds
  [Time delta from previous captured frame: 0.000190000 seconds]
  [Time delta from previous displayed frame: 0.018122000 seconds]
  [Time since reference or first frame: 185.280308000 seconds]
  Frame Number: 5165
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x5629 (22057)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x77ea [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60637 (60637), Seq: 279, Ack: 154, Len: 5
  Source port: http (80)
  Destination port: 60637 (60637)
  [Stream index: 193]
  Sequence number: 279    (relative sequence number)
  [Next sequence number: 284    (relative sequence number)]
  Acknowledgment number: 154    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0x2cba [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54413403, TSecr 16473297
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54413403
      Timestamp echo reply: 16473297
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (283 bytes): #5163(278), #5165(5)]
  [Frame: 5163, payload: 0-277 (278 bytes)]
  [Frame: 5165, payload: 278-282 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 283]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:06 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (118 octets)
      Chunk size: 118 octets
      Data (118 bytes)

0000  3c 61 20 68 72 65 66 3d 22 2f 63 6c 69 63 6b 2f   <a href="/click/
0010  64 65 66 63 35 30 35 64 34 38 38 65 30 61 30 30   defc505d488e0a00
0020  66 66 39 32 66 37 62 30 61 63 31 63 33 38 63 37   ff92f7b0ac1c38c7
0030  2f 34 33 63 66 65 35 61 61 66 36 66 35 33 33 32   /43cfe5aaf6f5332
0040  35 63 30 64 65 61 39 61 65 31 37 66 63 62 65 61   5c0dea9ae17fcbea
0050  63 22 3e 43 6c 69 63 6b 20 68 65 72 65 20 74 6f   c">Click here to
0060  20 77 69 6e 20 24 31 30 30 2c 30 30 30 2c 30 30    win $100,000,00
0070  30 21 3c 2f 61 3e                                 0!</a>
        Data: 3c6120687265663d222f636c69636b2f6465666335303564...
        [Length: 118]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <a href="/click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac">Click here to win $100,000,00
  0!</a>
```

```
No.     Time           Source                Destination           Protocol Length Info
   5203 186.639767000  10.0.1.51             171.66.3.23           HTTP     582    GET /click/defc505d488e0a00ff
92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac HTTP/1.1

Frame 5203: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:11.671187000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340411.671187000 seconds
  [Time delta from previous captured frame: 0.020324000 seconds]
  [Time delta from previous displayed frame: 1.359459000 seconds]
  [Time since reference or first frame: 186.639767000 seconds]
  Frame Number: 5203
  Frame Length: 582 bytes (4656 bits)
  Capture Length: 582 bytes (4656 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 566
  Identification: 0x4cf8 (19704)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x323e [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 5011, Ack: 2701, Len: 514
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 5011    (relative sequence number)
  [Next sequence number: 5525    (relative sequence number)]
  Acknowledgment number: 2701    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 198
  [Calculated window size: 25344]
  [Window size scaling factor: 128]
  Checksum: 0xa2f7 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16473711, TSecr 54410365
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16473711
      Timestamp echo reply: 54410365
  [SEQ/ACK analysis]
    [Bytes in flight: 514]
Hypertext Transfer Protocol
  GET /click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac HTTP/
    1.1\r\n]
      [Message: GET /click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcb
  eac]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5205 186.655993000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 5205: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:11.687413000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340411.687413000 seconds
  [Time delta from previous captured frame: 0.000230000 seconds]
  [Time delta from previous displayed frame: 0.016226000 seconds]
  [Time since reference or first frame: 186.655993000 seconds]
  Frame Number: 5205
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x1c26 (7206)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0xb1ed [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 2868, Ack: 5525, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 2868    (relative sequence number)
  [Next sequence number: 2873    (relative sequence number)]
  Acknowledgment number: 5525    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 206
  [Calculated window size: 26368]
  [Window size scaling factor: 128]
  Checksum: 0xd3e0 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54413815, TSecr 16473711
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54413815
      Timestamp echo reply: 16473711
  [SEQ/ACK analysis]
    [Bytes in flight: 172]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (172 bytes): #5204(167), #5205(5)]
  [Frame: 5204, payload: 0-166 (167 bytes)]
  [Frame: 5205, payload: 167-171 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 172]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:07 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (8 octets)
      Chunk size: 8 octets
      Data (8 bytes)

0000  53 75 63 63 65 73 73 21                           Success!
        Data: 5375636365737321
        [Length: 8]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  Success!
```

```
No.     Time           Source                Destination           Protocol Length Info
   5208 186.685468000  10.0.1.51             171.66.3.23           HTTP     556    GET /favicon.ico HTTP/1.1

Frame 5208: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:11.716888000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340411.716888000 seconds
  [Time delta from previous captured frame: 0.026451000 seconds]
  [Time delta from previous displayed frame: 0.029475000 seconds]
  [Time since reference or first frame: 186.685468000 seconds]
  Frame Number: 5208
  Frame Length: 556 bytes (4448 bits)
  Capture Length: 556 bytes (4448 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 540
  Identification: 0x4cfa (19706)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x3256 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 5525, Ack: 2873, Len: 488
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 5525    (relative sequence number)
  [Next sequence number: 6013    (relative sequence number)]
  Acknowledgment number: 2873    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 207
  [Calculated window size: 26496]
  [Window size scaling factor: 128]
  Checksum: 0x3a8e [validation disabled]
    [Good Checksum: False]
```

```
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16473724, TSecr 54413815
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16473724
      Timestamp echo reply: 54413815
  [SEQ/ACK analysis]
    [Bytes in flight: 488]
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      [Message: GET /favicon.ico HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /favicon.ico
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Referer: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/favicon.ico]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5215 186.723603000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 404 Not Found  (text
/html)

Frame 5215: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:11.755023000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340411.755023000 seconds
  [Time delta from previous captured frame: 0.000266000 seconds]
  [Time delta from previous displayed frame: 0.038135000 seconds]
  [Time since reference or first frame: 186.723603000 seconds]
  Frame Number: 5215
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x5767 (22375)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x76ac [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 3236, Ack: 6013, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 3236    (relative sequence number)
  [Next sequence number: 3241    (relative sequence number)]
  Acknowledgment number: 6013    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 214
  [Calculated window size: 27392]
  [Window size scaling factor: 128]
```

```
  Checksum: 0xd05e [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54413836, TSecr 16473724
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54413836
      Timestamp echo reply: 16473724
  [SEQ/ACK analysis]
    [Bytes in flight: 368]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (368 bytes): #5214(363), #5215(5)]
  [Frame: 5214, payload: 0-362 (363 bytes)]
  [Frame: 5215, payload: 363-367 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 368]
Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      [Message: HTTP/1.1 404 Not Found\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 404
    Response Phrase: Not Found
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:07 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (196 octets)
      Chunk size: 196 octets
      Data (196 bytes)

0000  3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50   <!DOCTYPE HTML P
0010  55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f   UBLIC "-//IETF//
0020  44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e   DTD HTML 2.0//EN
0030  22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a   ">.<HTML><HEAD>.
0040  3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46   <TITLE>404 Not F
0050  6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48   ound</TITLE>.</H
0060  45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e   EAD><BODY>.<H1>N
0070  6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 50   ot Found</H1>.<P
0080  3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55   >The requested U
0090  52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64   RL was not found
00a0  20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e    on this server.
00b0  3c 2f 50 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54   </P>.</BODY></HT
00c0  4d 4c 3e 0a                                       ML>.
        Data: 3c21444f4354595045204854 4d4c205055424c494320222d...
        [Length: 196]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <HTML><HEAD>\n
  <TITLE>404 Not Found</TITLE>\n
```

```
</HEAD><BODY>\n
<H1>Not Found</H1>\n
<P>The requested URL was not found on this server.</P>\n
</BODY></HTML>\n
```

```
No.     Time           Source                Destination           Protocol Length Info
   5314 190.797537000  10.0.1.51             171.66.3.23           HTTP     582    GET /click/defc505d488e0a00ff
92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac HTTP/1.1

Frame 5314: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:15.828957000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340415.828957000 seconds
  [Time delta from previous captured frame: 0.005162000 seconds]
  [Time delta from previous displayed frame: 4.073934000 seconds]
  [Time since reference or first frame: 190.797537000 seconds]
  Frame Number: 5314
  Frame Length: 582 bytes (4656 bits)
  Capture Length: 582 bytes (4656 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 566
  Identification: 0x4cfc (19708)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x323a [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 6013, Ack: 3241, Len: 514
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 6013    (relative sequence number)
  [Next sequence number: 6527    (relative sequence number)]
  Acknowledgment number: 3241    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 215
  [Calculated window size: 27520]
  [Window size scaling factor: 128]
  Checksum: 0x8a72 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16474958, TSecr 54413836
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16474958
      Timestamp echo reply: 54413836
  [SEQ/ACK analysis]
    [Bytes in flight: 514]
Hypertext Transfer Protocol
  GET /click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac HTTP/
    1.1\r\n]
      [Message: GET /click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcb
  eac]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5321 190.817480000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 400 Bad Request  (te
xt/html)

Frame 5321: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:15.848900000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340415.848900000 seconds
  [Time delta from previous captured frame: 0.000281000 seconds]
  [Time delta from previous displayed frame: 0.019943000 seconds]
  [Time since reference or first frame: 190.817480000 seconds]
  Frame Number: 5321
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x301b (12315)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x9df8 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 3600, Ack: 6527, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 3600    (relative sequence number)
  [Next sequence number: 3605    (relative sequence number)]
  Acknowledgment number: 6527    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 222
  [Calculated window size: 28416]
  [Window size scaling factor: 128]
```

```
  Checksum: 0xc34a [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54415064, TSecr 16474958
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54415064
      Timestamp echo reply: 16474958
  [SEQ/ACK analysis]
    [Bytes in flight: 364]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (364 bytes): #5320(359), #5321(5)]
  [Frame: 5320, payload: 0-358 (359 bytes)]
  [Frame: 5321, payload: 359-363 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 364]
Hypertext Transfer Protocol
  HTTP/1.1 400 Bad Request\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 400 Bad Request\r\n]
      [Message: HTTP/1.1 400 Bad Request\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 400
    Response Phrase: Bad Request
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:12 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (190 octets)
      Chunk size: 190 octets
      Data (190 bytes)

0000  3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50   <!DOCTYPE HTML P
0010  55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f   UBLIC "-//IETF//
0020  44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e   DTD HTML 2.0//EN
0030  22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a   ">.<HTML><HEAD>.
0040  3c 54 49 54 4c 45 3e 34 30 30 20 42 61 64 20 52   <TITLE>400 Bad R
0050  65 71 75 65 73 74 3c 2f 54 49 54 4c 45 3e 0a 3c   equest</TITLE>.<
0060  2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31   /HEAD><BODY>.<H1
0070  3e 42 61 64 20 52 65 71 75 65 73 74 3c 2f 48 31   >Bad Request</H1
0080  3e 0a 3c 50 3e 59 6f 75 72 20 72 65 71 75 65 73   >.<P>Your reques
0090  74 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 75   t could not be u
00a0  6e 64 65 72 73 74 6f 6f 64 2e 3c 2f 50 3e 0a 3c   nderstood.</P>.<
00b0  2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0a         /BODY></HTML>.
      Data: 3c21444f4354595045204854 4d4c205055424c494320222d...
      [Length: 190]
    Chunk boundary
  End of chunked encoding
    Chunk size: 0 octets
    Chunk boundary
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <HTML><HEAD>\n
  <TITLE>400 Bad Request</TITLE>\n
  </HEAD><BODY>\n
```

```
<H1>Bad Request</H1>\n
<P>Your request could not be understood.</P>\n
</BODY></HTML>\n
```

```
No.     Time           Source                Destination           Protocol Length Info
   5323 190.863178000  10.0.1.51             171.66.3.23           HTTP     556    GET /favicon.ico HTTP/1.1

Frame 5323: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:15.894598000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340415.894598000 seconds
  [Time delta from previous captured frame: 0.044852000 seconds]
  [Time delta from previous displayed frame: 0.045698000 seconds]
  [Time since reference or first frame: 190.863178000 seconds]
  Frame Number: 5323
  Frame Length: 556 bytes (4448 bits)
  Capture Length: 556 bytes (4448 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 540
  Identification: 0x4cfe (19710)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x3252 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 6527, Ack: 3605, Len: 488
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 6527    (relative sequence number)
  [Next sequence number: 7015    (relative sequence number)]
  Acknowledgment number: 3605    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 223
  [Calculated window size: 28544]
  [Window size scaling factor: 128]
  Checksum: 0x29f1 [validation disabled]
    [Good Checksum: False]
```

```
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16474978, TSecr 54415064
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16474978
      Timestamp echo reply: 54415064
  [SEQ/ACK analysis]
    [Bytes in flight: 488]
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      [Message: GET /favicon.ico HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /favicon.ico
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Referer: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/favicon.ico]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5325 190.877715000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 404 Not Found  (text
/html)

Frame 5325: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:15.909135000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340415.909135000 seconds
  [Time delta from previous captured frame: 0.000319000 seconds]
  [Time delta from previous displayed frame: 0.014537000 seconds]
  [Time since reference or first frame: 190.877715000 seconds]
  Frame Number: 5325
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x2e2c (11820)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x9fe7 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 3968, Ack: 7015, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 3968    (relative sequence number)
  [Next sequence number: 3973    (relative sequence number)]
  Acknowledgment number: 7015    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 231
  [Calculated window size: 29568]
  [Window size scaling factor: 128]
```

```
  Checksum: 0xbfc3 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54415082, TSecr 16474978
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54415082
      Timestamp echo reply: 16474978
  [SEQ/ACK analysis]
    [Bytes in flight: 368]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (368 bytes): #5324(363), #5325(5)]
  [Frame: 5324, payload: 0-362 (363 bytes)]
  [Frame: 5325, payload: 363-367 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 368]
Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      [Message: HTTP/1.1 404 Not Found\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 404
    Response Phrase: Not Found
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:12 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (196 octets)
      Chunk size: 196 octets
      Data (196 bytes)

0000  3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50   <!DOCTYPE HTML P
0010  55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f   UBLIC "-//IETF//
0020  44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e   DTD HTML 2.0//EN
0030  22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a   ">.<HTML><HEAD>.
0040  3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46   <TITLE>404 Not F
0050  6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48   ound</TITLE>.</H
0060  45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e   EAD><BODY>.<H1>N
0070  6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 50   ot Found</H1>.<P
0080  3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55   >The requested U
0090  52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64   RL was not found
00a0  20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e    on this server.
00b0  3c 2f 50 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54   </P>.</BODY></HT
00c0  4d 4c 3e 0a                                       ML>.
        Data: 3c21444f4354595045204854 4d4c205055424c494320222d...
        [Length: 196]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <HTML><HEAD>\n
  <TITLE>404 Not Found</TITLE>\n
```

```
</HEAD><BODY>\n
<H1>Not Found</H1>\n
<P>The requested URL was not found on this server.</P>\n
</BODY></HTML>\n
```

```
No.     Time           Source                Destination           Protocol Length Info
   5422 197.910776000  10.0.1.51             171.66.3.23           HTTP     582    GET /click/defc505d488e0a00ff
92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac HTTP/1.1

Frame 5422: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:22.942196000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340422.942196000 seconds
  [Time delta from previous captured frame: 0.026506000 seconds]
  [Time delta from previous displayed frame: 7.033061000 seconds]
  [Time since reference or first frame: 197.910776000 seconds]
  Frame Number: 5422
  Frame Length: 582 bytes (4656 bits)
  Capture Length: 582 bytes (4656 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 566
  Identification: 0x4d00 (19712)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x3236 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 7015, Ack: 3973, Len: 514
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 7015    (relative sequence number)
  [Next sequence number: 7529    (relative sequence number)]
  Acknowledgment number: 3973    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 232
  [Calculated window size: 29696]
  [Window size scaling factor: 128]
  Checksum: 0x7667 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16477092, TSecr 54415082
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16477092
      Timestamp echo reply: 54415082
  [SEQ/ACK analysis]
    [Bytes in flight: 514]
Hypertext Transfer Protocol
  GET /click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac HTTP/
    1.1\r\n]
      [Message: GET /click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcb
  eac]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5428 197.928527000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 400 Bad Request  (te
xt/html)

Frame 5428: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:22.959947000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340422.959947000 seconds
  [Time delta from previous captured frame: 0.000406000 seconds]
  [Time delta from previous displayed frame: 0.017751000 seconds]
  [Time since reference or first frame: 197.928527000 seconds]
  Frame Number: 5428
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xe562 (58722)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0xe8b0 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 4332, Ack: 7529, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 4332    (relative sequence number)
  [Next sequence number: 4337    (relative sequence number)]
  Acknowledgment number: 7529    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 239
  [Calculated window size: 30592]
  [Window size scaling factor: 128]
```

```
  Checksum: 0xabc8 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54417197, TSecr 16477092
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54417197
      Timestamp echo reply: 16477092
  [SEQ/ACK analysis]
    [Bytes in flight: 364]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (364 bytes): #5427(359), #5428(5)]
  [Frame: 5427, payload: 0-358 (359 bytes)]
  [Frame: 5428, payload: 359-363 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 364]
Hypertext Transfer Protocol
  HTTP/1.1 400 Bad Request\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 400 Bad Request\r\n]
      [Message: HTTP/1.1 400 Bad Request\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 400
    Response Phrase: Bad Request
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:19 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (190 octets)
      Chunk size: 190 octets
      Data (190 bytes)

0000  3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50   <!DOCTYPE HTML P
0010  55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f   UBLIC "-//IETF//
0020  44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e   DTD HTML 2.0//EN
0030  22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a   ">.<HTML><HEAD>.
0040  3c 54 49 54 4c 45 3e 34 30 30 20 42 61 64 20 52   <TITLE>400 Bad R
0050  65 71 75 65 73 74 3c 2f 54 49 54 4c 45 3e 0a 3c   equest</TITLE>.<
0060  2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31   /HEAD><BODY>.<H1
0070  3e 42 61 64 20 52 65 71 75 65 73 74 3c 2f 48 31   >Bad Request</H1
0080  3e 0a 3c 50 3e 59 6f 75 72 20 72 65 71 75 65 73   >.<P>Your reques
0090  74 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 75   t could not be u
00a0  6e 64 65 72 73 74 6f 6f 64 2e 3c 2f 50 3e 0a 3c   nderstood.</P>.<
00b0  2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0a         /BODY></HTML>.
      Data: 3c21444f4354595045204854 4d4c205055424c494320222d...
      [Length: 190]
    Chunk boundary
  End of chunked encoding
    Chunk size: 0 octets
    Chunk boundary
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <HTML><HEAD>\n
  <TITLE>400 Bad Request</TITLE>\n
  </HEAD><BODY>\n
```

```
<H1>Bad Request</H1>\n
<P>Your request could not be understood.</P>\n
</BODY></HTML>\n
```

```
No.     Time           Source                Destination           Protocol Length Info
   5430 197.954007000  10.0.1.51             171.66.3.23           HTTP     556    GET /favicon.ico HTTP/1.1

Frame 5430: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:22.985427000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340422.985427000 seconds
  [Time delta from previous captured frame: 0.021797000 seconds]
  [Time delta from previous displayed frame: 0.025480000 seconds]
  [Time since reference or first frame: 197.954007000 seconds]
  Frame Number: 5430
  Frame Length: 556 bytes (4448 bits)
  Capture Length: 556 bytes (4448 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 540
  Identification: 0x4d02 (19714)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x324e [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 7529, Ack: 4337, Len: 488
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 7529    (relative sequence number)
  [Next sequence number: 8017    (relative sequence number)]
  Acknowledgment number: 4337    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 240
  [Calculated window size: 30720]
  [Window size scaling factor: 128]
  Checksum: 0x1276 [validation disabled]
    [Good Checksum: False]
```

```
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16477105, TSecr 54417197
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16477105
      Timestamp echo reply: 54417197
  [SEQ/ACK analysis]
    [Bytes in flight: 488]
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      [Message: GET /favicon.ico HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /favicon.ico
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Referer: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/43cfe5aaf6f53325c0dea9ae17fcbeac\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/favicon.ico]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5433 197.970720000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 404 Not Found  (text
/html)

Frame 5433: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:23.002140000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340423.002140000 seconds
  [Time delta from previous captured frame: 0.000787000 seconds]
  [Time delta from previous displayed frame: 0.016713000 seconds]
  [Time since reference or first frame: 197.970720000 seconds]
  Frame Number: 5433
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xfd52 (64850)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0xd0c0 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 4700, Ack: 8017, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 4700    (relative sequence number)
  [Next sequence number: 4705    (relative sequence number)]
  Acknowledgment number: 8017    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 248
  [Calculated window size: 31744]
  [Window size scaling factor: 128]
```

```
  Checksum: 0xa84d [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54417210, TSecr 16477105
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54417210
      Timestamp echo reply: 16477105
  [SEQ/ACK analysis]
    [Bytes in flight: 368]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (368 bytes): #5432(363), #5433(5)]
  [Frame: 5432, payload: 0-362 (363 bytes)]
  [Frame: 5433, payload: 363-367 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 368]
Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      [Message: HTTP/1.1 404 Not Found\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 404
    Response Phrase: Not Found
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:19 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (196 octets)
      Chunk size: 196 octets
      Data (196 bytes)

0000  3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50   <!DOCTYPE HTML P
0010  55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f   UBLIC "-//IETF//
0020  44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e   DTD HTML 2.0//EN
0030  22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a   ">.<HTML><HEAD>.
0040  3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46   <TITLE>404 Not F
0050  6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48   ound</TITLE>.</H
0060  45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e   EAD><BODY>.<H1>N
0070  6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 50   ot Found</H1>.<P
0080  3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55   >The requested U
0090  52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64   RL was not found
00a0  20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e    on this server.
00b0  3c 2f 50 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54   </P>.</BODY></HT
00c0  4d 4c 3e 0a                                       ML>.
        Data: 3c21444f4354595045204854 4d4c205055424c494320222d...
        [Length: 196]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <HTML><HEAD>\n
  <TITLE>404 Not Found</TITLE>\n
```

```
</HEAD><BODY>\n
<H1>Not Found</H1>\n
<P>The requested URL was not found on this server.</P>\n
</BODY></HTML>\n
```

```
No.     Time           Source                Destination           Protocol Length Info
   5541 203.817726000  10.0.1.51             171.66.3.23           HTTP     221    GET /token?keywords=java&app_
id=9469ea8ba22b4786f382986111518038 HTTP/1.1

Frame 5541: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:28.849146000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340428.849146000 seconds
  [Time delta from previous captured frame: 0.005380000 seconds]
  [Time delta from previous displayed frame: 5.847006000 seconds]
  [Time since reference or first frame: 203.817726000 seconds]
  Frame Number: 5541
  Frame Length: 221 bytes (1768 bits)
  Capture Length: 221 bytes (1768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 205
  Identification: 0x6ecc (28364)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x11d3 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60644 (60644), Dst Port: http (80), Seq: 1, Ack: 1, Len: 153
  Source port: 60644 (60644)
  Destination port: http (80)
  [Stream index: 201]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 154    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0xdebc [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16478864, TSecr 54418947
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16478864
      Timestamp echo reply: 54418947
  [SEQ/ACK analysis]
    [Bytes in flight: 153]
Hypertext Transfer Protocol
  GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Message: GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: Keep-Alive\r\n
  User-Agent: adlib-android\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/token?keywords=java&app_id=9469ea8ba22b4786f382986111518038]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5545 203.840068000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 5545: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:28.871488000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340428.871488000 seconds
  [Time delta from previous captured frame: 0.000112000 seconds]
  [Time delta from previous displayed frame: 0.022342000 seconds]
  [Time since reference or first frame: 203.840068000 seconds]
  Frame Number: 5545
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xbd66 (48486)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x10ad [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60644 (60644), Seq: 279, Ack: 154, Len: 5
  Source port: http (80)
  Destination port: 60644 (60644)
  [Stream index: 201]
  Sequence number: 279    (relative sequence number)
  [Next sequence number: 284    (relative sequence number)]
  Acknowledgment number: 154    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0x4e88 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54418968, TSecr 16478864
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54418968
      Timestamp echo reply: 16478864
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (283 bytes): #5543(278), #5545(5)]
  [Frame: 5543, payload: 0-277 (278 bytes)]
  [Frame: 5545, payload: 278-282 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 283]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:25 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (118 octets)
      Chunk size: 118 octets
      Data (118 bytes)

0000  3c 61 20 68 72 65 66 3d 22 2f 63 6c 69 63 6b 2f   <a href="/click/
0010  64 65 66 63 35 30 35 64 34 38 38 65 30 61 30 30   defc505d488e0a00
0020  66 66 39 32 66 37 62 30 61 63 31 63 33 38 63 37   ff92f7b0ac1c38c7
0030  2f 38 35 61 64 39 38 31 32 37 34 33 34 64 66 63   /85ad98127434dfc
0040  64 37 62 38 32 65 62 34 32 63 37 66 62 37 38 31   d7b82eb42c7fb781
0050  66 22 3e 43 6c 69 63 6b 20 68 65 72 65 20 74 6f   f">Click here to
0060  20 77 69 6e 20 24 31 30 30 2c 30 30 30 2c 30 30    win $100,000,00
0070  30 21 3c 2f 61 3e                                 0!</a>
        Data: 3c6120687265663d222f636c69636b2f6465666335303564...
        [Length: 118]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <a href="/click/defc505d488e0a00ff92f7b0ac1c38c7/85ad98127434dfcd7b82eb42c7fb781f">Click here to win $100,000,00
  0!</a>
```

```
No.     Time           Source                Destination           Protocol Length Info
   5586 205.779217000  10.0.1.51             171.66.3.23           HTTP     582    GET /click/defc505d488e0a00ff
92f7b0ac1c38c7/85ad98127434dfcd7b82eb42c7fb781f HTTP/1.1

Frame 5586: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:30.810637000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340430.810637000 seconds
  [Time delta from previous captured frame: 0.035785000 seconds]
  [Time delta from previous displayed frame: 1.939149000 seconds]
  [Time since reference or first frame: 205.779217000 seconds]
  Frame Number: 5586
  Frame Length: 582 bytes (4656 bits)
  Capture Length: 582 bytes (4656 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 566
  Identification: 0x4d04 (19716)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x3232 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 8017, Ack: 4705, Len: 514
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 8017    (relative sequence number)
  [Next sequence number: 8531    (relative sequence number)]
  Acknowledgment number: 4705    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 249
  [Calculated window size: 31872]
  [Window size scaling factor: 128]
  Checksum: 0x620b [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16479453, TSecr 54417210
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16479453
      Timestamp echo reply: 54417210
  [SEQ/ACK analysis]
    [Bytes in flight: 514]
Hypertext Transfer Protocol
  GET /click/defc505d488e0a00ff92f7b0ac1c38c7/85ad98127434dfcd7b82eb42c7fb781f HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /click/defc505d488e0a00ff92f7b0ac1c38c7/85ad98127434dfcd7b82eb42c7fb781f HTTP/
    1.1\r\n]
      [Message: GET /click/defc505d488e0a00ff92f7b0ac1c38c7/85ad98127434dfcd7b82eb42c7fb781f HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /click/defc505d488e0a00ff92f7b0ac1c38c7/85ad98127434dfcd7b82eb42c7fb781f
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/85ad98127434dfcd7b82eb42c7fb7
  81f]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5594 205.805548000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 5594: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:30.836968000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340430.836968000 seconds
  [Time delta from previous captured frame: 0.000269000 seconds]
  [Time delta from previous displayed frame: 0.026331000 seconds]
  [Time since reference or first frame: 205.805548000 seconds]
  Frame Number: 5594
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xc708 (50952)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x070b [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 4872, Ack: 8531, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 4872    (relative sequence number)
  [Next sequence number: 4877    (relative sequence number)]
  Acknowledgment number: 8531    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 256
  [Calculated window size: 32768]
  [Window size scaling factor: 128]
  Checksum: 0x933f [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54419558, TSecr 16479453
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54419558
      Timestamp echo reply: 16479453
  [SEQ/ACK analysis]
    [Bytes in flight: 172]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (172 bytes): #5593(167), #5594(5)]
  [Frame: 5593, payload: 0-166 (167 bytes)]
  [Frame: 5594, payload: 167-171 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 172]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:27 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (8 octets)
      Chunk size: 8 octets
      Data (8 bytes)

0000  53 75 63 63 65 73 73 21                           Success!
        Data: 5375636365737321
        [Length: 8]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  Success!
```

```
No.     Time           Source                Destination           Protocol Length Info
   5596 205.825653000  10.0.1.51             171.66.3.23           HTTP     556    GET /favicon.ico HTTP/1.1

Frame 5596: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:30.857073000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340430.857073000 seconds
  [Time delta from previous captured frame: 0.017325000 seconds]
  [Time delta from previous displayed frame: 0.020105000 seconds]
  [Time since reference or first frame: 205.825653000 seconds]
  Frame Number: 5596
  Frame Length: 556 bytes (4448 bits)
  Capture Length: 556 bytes (4448 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 540
  Identification: 0x4d06 (19718)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x324a [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 8531, Ack: 4877, Len: 488
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 8531    (relative sequence number)
  [Next sequence number: 9019    (relative sequence number)]
  Acknowledgment number: 4877    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 257
  [Calculated window size: 32896]
  [Window size scaling factor: 128]
  Checksum: 0xfdf0 [validation disabled]
    [Good Checksum: False]
```

```
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16479466, TSecr 54419558
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16479466
      Timestamp echo reply: 54419558
  [SEQ/ACK analysis]
    [Bytes in flight: 488]
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      [Message: GET /favicon.ico HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /favicon.ico
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Referer: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/85ad98127434dfcd7b82eb42c7fb781f\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/favicon.ico]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5598 205.839271000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 404 Not Found  (text
/html)

Frame 5598: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:30.870691000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340430.870691000 seconds
  [Time delta from previous captured frame: 0.000273000 seconds]
  [Time delta from previous displayed frame: 0.013618000 seconds]
  [Time since reference or first frame: 205.839271000 seconds]
  Frame Number: 5598
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xfa3b (64059)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0xd3d7 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 5240, Ack: 9019, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 5240    (relative sequence number)
  [Next sequence number: 5245    (relative sequence number)]
  Acknowledgment number: 9019    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 264
  [Calculated window size: 33792]
  [Window size scaling factor: 128]
```

```
  Checksum: 0x8fc6 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54419570, TSecr 16479466
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54419570
      Timestamp echo reply: 16479466
  [SEQ/ACK analysis]
    [Bytes in flight: 368]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (368 bytes): #5597(363), #5598(5)]
  [Frame: 5597, payload: 0-362 (363 bytes)]
  [Frame: 5598, payload: 363-367 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 368]
Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      [Message: HTTP/1.1 404 Not Found\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 404
    Response Phrase: Not Found
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:27 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (196 octets)
      Chunk size: 196 octets
      Data (196 bytes)

0000  3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50   <!DOCTYPE HTML P
0010  55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f   UBLIC "-//IETF//
0020  44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e   DTD HTML 2.0//EN
0030  22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a   ">.<HTML><HEAD>.
0040  3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46   <TITLE>404 Not F
0050  6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48   ound</TITLE>.</H
0060  45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e   EAD><BODY>.<H1>N
0070  6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 50   ot Found</H1>.<P
0080  3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55   >The requested U
0090  52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64   RL was not found
00a0  20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e    on this server.
00b0  3c 2f 50 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54   </P>.</BODY></HT
00c0  4d 4c 3e 0a                                       ML>.
        Data: 3c21444f4354595045204854 4d4c205055424c494320222d...
        [Length: 196]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <HTML><HEAD>\n
  <TITLE>404 Not Found</TITLE>\n
```

```
</HEAD><BODY>\n
<H1>Not Found</H1>\n
<P>The requested URL was not found on this server.</P>\n
</BODY></HTML>\n
```

```
No.     Time           Source                Destination           Protocol Length Info
   5709 213.643377000  10.0.1.51             171.66.3.23           HTTP     221    GET /token?keywords=java&app_
id=9469ea8ba22b4786f382986111518038 HTTP/1.1

Frame 5709: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:38.674797000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340438.674797000 seconds
  [Time delta from previous captured frame: 0.014666000 seconds]
  [Time delta from previous displayed frame: 7.804106000 seconds]
  [Time since reference or first frame: 213.643377000 seconds]
  Frame Number: 5709
  Frame Length: 221 bytes (1768 bits)
  Capture Length: 221 bytes (1768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 205
  Identification: 0x12de (4830)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x6dc1 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60649 (60649), Dst Port: http (80), Seq: 1, Ack: 1, Len: 153
  Source port: 60649 (60649)
  Destination port: http (80)
  [Stream index: 206]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 154    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0x8c65 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16481812, TSecr 54421907
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16481812
      Timestamp echo reply: 54421907
  [SEQ/ACK analysis]
    [Bytes in flight: 153]
Hypertext Transfer Protocol
  GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Message: GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: Keep-Alive\r\n
  User-Agent: adlib-android\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/token?keywords=java&app_id=9469ea8ba22b4786f382986111518038]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5714 213.669859000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 5714: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:38.701279000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340438.701279000 seconds
  [Time delta from previous captured frame: 0.007515000 seconds]
  [Time delta from previous displayed frame: 0.026482000 seconds]
  [Time since reference or first frame: 213.669859000 seconds]
  Frame Number: 5714
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0xc331 (49969)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x0ae2 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60649 (60649), Seq: 279, Ack: 154, Len: 5
  Source port: http (80)
  Destination port: 60649 (60649)
  [Stream index: 206]
  Sequence number: 279    (relative sequence number)
  [Next sequence number: 284    (relative sequence number)]
  Acknowledgment number: 154    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0xfc3c [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54421916, TSecr 16481812
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54421916
      Timestamp echo reply: 16481812
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (283 bytes): #5711(278), #5714(5)]
  [Frame: 5711, payload: 0-277 (278 bytes)]
  [Frame: 5714, payload: 278-282 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 283]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:34 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (118 octets)
      Chunk size: 118 octets
      Data (118 bytes)

0000  3c 61 20 68 72 65 66 3d 22 2f 63 6c 69 63 6b 2f   <a href="/click/
0010  64 65 66 63 35 30 35 64 34 38 38 65 30 61 30 30   defc505d488e0a00
0020  66 66 39 32 66 37 62 30 61 63 31 63 33 38 63 37   ff92f7b0ac1c38c7
0030  2f 34 65 31 39 63 66 62 39 65 61 66 37 65 30 35   /4e19cfb9eaf7e05
0040  36 35 37 39 31 37 61 64 39 61 33 64 37 38 38 63   657917ad9a3d788c
0050  37 22 3e 43 6c 69 63 6b 20 68 65 72 65 20 74 6f   7">Click here to
0060  20 77 69 6e 20 24 31 30 30 2c 30 30 30 2c 30 30    win $100,000,00
0070  30 21 3c 2f 61 3e                                 0!</a>
      Data: 3c6120687265663d222f636c69636b2f6465666335303564...
      [Length: 118]
    Chunk boundary
  End of chunked encoding
    Chunk size: 0 octets
    Chunk boundary
Line-based text data: text/html
  <a href="/click/defc505d488e0a00ff92f7b0ac1c38c7/4e19cfb9eaf7e05657917ad9a3d788c7">Click here to win $100,000,00
  0!</a>
```

```
No.     Time           Source                Destination           Protocol Length Info
   5774 218.532389000  10.0.1.51             171.66.3.23           HTTP     221    GET /token?keywords=java&app_
id=9469ea8ba22b4786f382986111518038 HTTP/1.1

Frame 5774: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:43.563809000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340443.563809000 seconds
  [Time delta from previous captured frame: 0.006713000 seconds]
  [Time delta from previous displayed frame: 4.862530000 seconds]
  [Time since reference or first frame: 218.532389000 seconds]
  Frame Number: 5774
  Frame Length: 221 bytes (1768 bits)
  Capture Length: 221 bytes (1768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 205
  Identification: 0xd30f (54031)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0xad8f [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60651 (60651), Dst Port: http (80), Seq: 1, Ack: 1, Len: 153
  Source port: 60651 (60651)
  Destination port: http (80)
  [Stream index: 208]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 154    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 115
  [Calculated window size: 14720]
  [Window size scaling factor: 128]
  Checksum: 0x1cb9 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16483279, TSecr 54423376
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16483279
      Timestamp echo reply: 54423376
  [SEQ/ACK analysis]
    [Bytes in flight: 153]
Hypertext Transfer Protocol
  GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Message: GET /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038 HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /token?keywords=java&app_id=9469ea8ba22b4786f382986111518038
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: Keep-Alive\r\n
  User-Agent: adlib-android\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/token?keywords=java&app_id=9469ea8ba22b4786f382986111518038]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5778 218.552176000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 5778: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:43.583596000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340443.583596000 seconds
  [Time delta from previous captured frame: 0.000495000 seconds]
  [Time delta from previous displayed frame: 0.019787000 seconds]
  [Time since reference or first frame: 218.552176000 seconds]
  Frame Number: 5778
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x663e (26174)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x67d5 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60651 (60651), Seq: 279, Ack: 154, Len: 5
  Source port: http (80)
  Destination port: 60651 (60651)
  [Stream index: 208]
  Sequence number: 279    (relative sequence number)
  [Next sequence number: 284    (relative sequence number)]
  Acknowledgment number: 154    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 122
  [Calculated window size: 15616]
  [Window size scaling factor: 128]
  Checksum: 0x8c92 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54423383, TSecr 16483279
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54423383
      Timestamp echo reply: 16483279
  [SEQ/ACK analysis]
    [Bytes in flight: 5]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (283 bytes): #5776(278), #5778(5)]
  [Frame: 5776, payload: 0-277 (278 bytes)]
  [Frame: 5778, payload: 278-282 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 283]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:39 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (118 octets)
      Chunk size: 118 octets
      Data (118 bytes)

0000  3c 61 20 68 72 65 66 3d 22 2f 63 6c 69 63 6b 2f   <a href="/click/
0010  64 65 66 63 35 30 35 64 34 38 38 65 30 61 30 30   defc505d488e0a00
0020  66 66 39 32 66 37 62 30 61 63 31 63 33 38 63 37   ff92f7b0ac1c38c7
0030  2f 34 39 62 33 34 36 61 66 65 34 30 66 30 66 66   /49b346afe40f0ff
0040  30 39 65 39 37 31 33 39 63 35 63 30 39 64 33 30   09e97139c5c09d30
0050  62 22 3e 43 6c 69 63 6b 20 68 65 72 65 20 74 6f   b">Click here to
0060  20 77 69 6e 20 24 31 30 30 2c 30 30 30 2c 30 30    win $100,000,00
0070  30 21 3c 2f 61 3e                                 0!</a>
        Data: 3c6120687265663d222f636c69636b2f6465666335303564...
        [Length: 118]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <a href="/click/defc505d488e0a00ff92f7b0ac1c38c7/49b346afe40f0ff09e97139c5c09d30b">Click here to win $100,000,00
  0!</a>
```

```
No.     Time           Source                Destination           Protocol Length Info
   5820 220.492954000  10.0.1.51             171.66.3.23           HTTP     582    GET /click/defc505d488e0a00ff
92f7b0ac1c38c7/49b346afe40f0ff09e97139c5c09d30b HTTP/1.1

Frame 5820: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:45.524374000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340445.524374000 seconds
  [Time delta from previous captured frame: 0.028921000 seconds]
  [Time delta from previous displayed frame: 1.940778000 seconds]
  [Time since reference or first frame: 220.492954000 seconds]
  Frame Number: 5820
  Frame Length: 582 bytes (4656 bits)
  Capture Length: 582 bytes (4656 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 566
  Identification: 0x4d08 (19720)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x322e [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 9019, Ack: 5245, Len: 514
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 9019    (relative sequence number)
  [Next sequence number: 9533    (relative sequence number)]
  Acknowledgment number: 5245    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 265
  [Calculated window size: 33920]
  [Window size scaling factor: 128]
  Checksum: 0x8378 [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16483867, TSecr 54419570
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16483867
      Timestamp echo reply: 54419570
  [SEQ/ACK analysis]
    [Bytes in flight: 514]
Hypertext Transfer Protocol
  GET /click/defc505d488e0a00ff92f7b0ac1c38c7/49b346afe40f0ff09e97139c5c09d30b HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /click/defc505d488e0a00ff92f7b0ac1c38c7/49b346afe40f0ff09e97139c5c09d30b HTTP/
    1.1\r\n]
      [Message: GET /click/defc505d488e0a00ff92f7b0ac1c38c7/49b346afe40f0ff09e97139c5c09d30b HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /click/defc505d488e0a00ff92f7b0ac1c38c7/49b346afe40f0ff09e97139c5c09d30b
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/49b346afe40f0ff09e97139c5c09d
  30b]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5828 220.508211000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 200 OK  (text/html)

Frame 5828: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:45.539631000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340445.539631000 seconds
  [Time delta from previous captured frame: 0.000221000 seconds]
  [Time delta from previous displayed frame: 0.015257000 seconds]
  [Time since reference or first frame: 220.508211000 seconds]
  Frame Number: 5828
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x3135 (12597)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x9cde [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 5412, Ack: 9533, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 5412    (relative sequence number)
  [Next sequence number: 5417    (relative sequence number)]
  Acknowledgment number: 9533    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 273
  [Calculated window size: 34944]
  [Window size scaling factor: 128]
  Checksum: 0x6aad [validation disabled]
```

```
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54423971, TSecr 16483867
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54423971
      Timestamp echo reply: 16483867
  [SEQ/ACK analysis]
    [Bytes in flight: 172]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (172 bytes): #5827(167), #5828(5)]
  [Frame: 5827, payload: 0-166 (167 bytes)]
  [Frame: 5828, payload: 167-171 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 172]
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
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:41 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (8 octets)
      Chunk size: 8 octets
      Data (8 bytes)

0000  53 75 63 63 65 73 73 21                           Success!
        Data: 5375636365737321
        [Length: 8]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  Success!
```

```
No.     Time           Source                Destination           Protocol Length Info
   5830 220.539940000  10.0.1.51             171.66.3.23           HTTP     556    GET /favicon.ico HTTP/1.1

Frame 5830: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:45.571360000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340445.571360000 seconds
  [Time delta from previous captured frame: 0.025331000 seconds]
  [Time delta from previous displayed frame: 0.031729000 seconds]
  [Time since reference or first frame: 220.539940000 seconds]
  Frame Number: 5830
  Frame Length: 556 bytes (4448 bits)
  Capture Length: 556 bytes (4448 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Sent by us (4)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: IntelCor_ae:35:00 (60:67:20:ae:35:00)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.1.51 (10.0.1.51), Dst: 171.66.3.23 (171.66.3.23)
  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: 540
  Identification: 0x4d0a (19722)
  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: 64
  Protocol: TCP (6)
  Header checksum: 0x3246 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.0.1.51 (10.0.1.51)
  Destination: 171.66.3.23 (171.66.3.23)
Transmission Control Protocol, Src Port: 60611 (60611), Dst Port: http (80), Seq: 9533, Ack: 5417, Len: 488
  Source port: 60611 (60611)
  Destination port: http (80)
  [Stream index: 167]
  Sequence number: 9533    (relative sequence number)
  [Next sequence number: 10021    (relative sequence number)]
  Acknowledgment number: 5417    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 274
  [Calculated window size: 35072]
  [Window size scaling factor: 128]
  Checksum: 0xce9f [validation disabled]
    [Good Checksum: False]
```

```
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 16483881, TSecr 54423971
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 16483881
      Timestamp echo reply: 54423971
  [SEQ/ACK analysis]
    [Bytes in flight: 488]
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      [Message: GET /favicon.ico HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /favicon.ico
    Request Version: HTTP/1.1
  Host: adlib.mappend.net\r\n
  Connection: keep-alive\r\n
  Referer: http://adlib.mappend.net/click/defc505d488e0a00ff92f7b0ac1c38c7/49b346afe40f0ff09e97139c5c09d30b\r\n
  X-Requested-With: com.android.browser\r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; google_sdk Build/JB_MR1.1) AppleWebKit/534.30 (KHTML, l
  ike Gecko) Version/4.0 Mobile Safari/534.30\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Language: en-US\r\n
  Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
  \r\n
  [Full request URI: http://adlib.mappend.net/favicon.ico]
```

```
No.     Time           Source                Destination           Protocol Length Info
   5832 220.556339000  171.66.3.23           10.0.1.51             HTTP     73     HTTP/1.1 404 Not Found  (text
/html)

Frame 5832: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 25
  Arrival Time: May 23, 2013 13:20:45.587759000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1369340445.587759000 seconds
  [Time delta from previous captured frame: 0.000243000 seconds]
  [Time delta from previous displayed frame: 0.016399000 seconds]
  [Time since reference or first frame: 220.556339000 seconds]
  Frame Number: 5832
  Frame Length: 73 bytes (584 bits)
  Capture Length: 73 bytes (584 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ip:tcp:http:data:data:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Linux cooked capture
  Packet type: Unicast to us (0)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Apple_6b:4f:d5 (00:26:bb:6b:4f:d5)
  Protocol: IP (0x0800)
Internet Protocol Version 4, Src: 171.66.3.23 (171.66.3.23), Dst: 10.0.1.51 (10.0.1.51)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)
  )
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 57
  Identification: 0x756f (30063)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 51
  Protocol: TCP (6)
  Header checksum: 0x58a4 [correct]
    [Good: True]
    [Bad: False]
  Source: 171.66.3.23 (171.66.3.23)
  Destination: 10.0.1.51 (10.0.1.51)
Transmission Control Protocol, Src Port: http (80), Dst Port: 60611 (60611), Seq: 5780, Ack: 10021, Len: 5
  Source port: http (80)
  Destination port: 60611 (60611)
  [Stream index: 167]
  Sequence number: 5780    (relative sequence number)
  [Next sequence number: 5785    (relative sequence number)]
  Acknowledgment number: 10021    (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (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 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 281
  [Calculated window size: 35968]
  [Window size scaling factor: 128]
```

```
  Checksum: 0x6731 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    No-Operation (NOP)
      Type: 1
        0... .... = Copy on fragmentation: No
        .00. .... = Class: Control (0)
        ...0 0001 = Number: No-Operation (NOP) (1)
    Timestamps: TSval 54423985, TSecr 16483881
      Kind: Timestamp (8)
      Length: 10
      Timestamp value: 54423985
      Timestamp echo reply: 16483881
  [SEQ/ACK analysis]
    [Bytes in flight: 368]
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (368 bytes): #5831(363), #5832(5)]
  [Frame: 5831, payload: 0-362 (363 bytes)]
  [Frame: 5832, payload: 363-367 (5 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 368]
Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      [Message: HTTP/1.1 404 Not Found\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 404
    Response Phrase: Not Found
  Server: nginx/1.4.1\r\n
  Date: Thu, 23 May 2013 20:21:41 GMT\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  \r\n
  HTTP chunked response
    Data chunk (196 octets)
      Chunk size: 196 octets
      Data (196 bytes)

0000  3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50   <!DOCTYPE HTML P
0010  55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f   UBLIC "-//IETF//
0020  44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e   DTD HTML 2.0//EN
0030  22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a   ">.<HTML><HEAD>.
0040  3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46   <TITLE>404 Not F
0050  6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48   ound</TITLE>.</H
0060  45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e   EAD><BODY>.<H1>N
0070  6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 50   ot Found</H1>.<P
0080  3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55   >The requested U
0090  52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64   RL was not found
00a0  20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e    on this server.
00b0  3c 2f 50 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54   </P>.</BODY></HT
00c0  4d 4c 3e 0a                                       ML>.
        Data: 3c21444f4354595045204854 4d4c205055424c494320222d...
        [Length: 196]
      Chunk boundary
    End of chunked encoding
      Chunk size: 0 octets
      Chunk boundary
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <HTML><HEAD>\n
  <TITLE>404 Not Found</TITLE>\n
```

```
</HEAD><BODY>\n
<H1>Not Found</H1>\n
<P>The requested URL was not found on this server.</P>\n
</BODY></HTML>\n
```