

## LAB 05 WIRESHARK2

|               |                                 |
|---------------|---------------------------------|
| Name          | Tran Dang Khoa                  |
| Email address | Khoab2014926@student.ctu.edu.vn |
| Class         | MO2                             |
| Browser       | Safari, Chrome, IE, Firefox     |

**Design** Wireshark analyzing **scenario under Windows**

|                  | scanner            | target   |
|------------------|--------------------|--|
| OS               | Windows<br>Ubuntu  | Windows, Linux   |
| IP address       | Test - bed host IP | Localhost<br>CTU IP<br>CICT IP<br>Neighboring PC IP<br>VM IP(Ubuntu, Centos) |
| scanning program | Wireshark          |  |
| scanning types   | filter HTTP        |  |

HTTP executing scenario

- 1 (browser) Visit one website

**HỆ THỐNG QUẢN LÝ**

Trang chủ

**ĐĂNG NHẬP**

Mã bảo vệ T 9 a Z Z

**ĐĂNG NHẬP**

Chú ý:

- Mã bảo vệ là nhập các ký tự trên hình **phía bên phải** của ô mã bảo vệ.
- Sinh viên đăng nhập vào Hệ thống quản lý của Trường từ máy tính bên ngoài Trường Đại Học Cần Thơ vui lòng nhấn **vào đây**

**THÔNG BÁO MỚI NHẤT**

- Thông báo đưa, đón SV K49 học thực hành GDQP đợt 1 học kỳ 1, năm học 2023-2024
- Thông báo mức học phí năm học 2023-2024
- Thông báo lịch học GDQP&AN khóa 49 học kỳ 1, năm học 2023-2024
- Thông báo mở lại website kế hoạch học tập
- Thông báo xóa lớp học phần HK1, năm học 2023-2024 (Đợt 2)
- Thông báo xóa lớp học phần HK1, năm học 2023-2024 (Đợt 1)
- Thông báo kế hoạch giảng dạy và đăng ký học phần HK1, 2023-2024
- Thông báo đưa, đón SV K48 học thực hành GDQP đợt 2 (đợt cuối) học kỳ 3, năm học 2022-2023
- Thông báo xóa lớp học phần HK3, năm học 2022-2023 (Đợt 1)
- Thông báo đưa, đón SV K48 học thực hành GDQP đợt 1 học kỳ 3, năm học 2022-2023
- Thông báo lịch học GDQP&AN khóa 48 học kỳ 3, năm học 2022-2023 (Điều chỉnh)
- Thông báo kế hoạch giảng dạy và đăng ký học phần HK3, 2022-2023
- Thông báo đưa, đón SV K48 học thực hành GDQP đợt 5 (đợt cuối) học kỳ 2, năm học 2022-2023
- Thông báo đưa, đón SV K48 học thực hành GDQP đợt 4 học kỳ 2, năm học 2022-2023
- Thông báo đưa, đón SV K48 học thực hành GDQP đợt 3 học kỳ 2, năm học 2022-2023
- Thông báo đưa, đón SV K48 học thực hành GDQP đợt 2 học kỳ 2, năm học 2022-2023
- Thông báo mở lại website KHHT.
- Thông báo xóa các lớp học phần HK2, năm học 2022-2023 (Đợt cuối)

2 (website) Log in to home page

**HỆ THỐNG QUẢN LÝ**

Thoát

Trang chủ

Trần Đăng Khoa (B2014926)

**THÔNG TIN SINH VIÊN**

|           |   |
|-----------|---|
| Mã SV     | B2014926                                  |
| Họ tên    | Trần Đăng Khoa                            |
| Ngày sinh | 15/08/2002                                |
| Giới tính | Nam                                       |
| Lớp       | DI20V7F2                                  |
| Ngành học | Công nghệ thông tin                       |
| Khóa học  | 46 (2020)                                 |
| Khoa      | Trường Công nghệ Thông tin & Truyền thông |

Xem thêm...  
 Cập nhật thông tin

Kế hoạch học tập

Kết quả học tập

Nghiên cứu khoa học

Hệ thống lấy ý kiến trực tuyến

Đoàn viên

Đánh giá rèn luyện

Đăng ký học phần

Kết quả tốt nghiệp

Ký túc xá

Hoạt động ngoại khóa

Đăng ký ngành 2

Phòng học

3 (browser) find input string on URL box

dknh.ctu.edu.vn/htql/sinhvien/hindex.php

4 (wireshark) choose one packet

Apply a display filter ... Ctrl+F

| No.   | Time      | Source         | Destination    | Protocol | Length | Info  |
|-------|-----------|----------------|----------------|----------|--------|---|
| 22670 | 41.788707 | 113.171.237.82 | 10.2.10.51     | UDP      | 1292   | 443 → 58427 Len=1250  |
| 22671 | 41.789549 | 10.2.10.51     | 113.171.237.82 | UDP      | 78     | 58427 → 443 Len=36  |
| 22672 | 41.866472 | 113.171.237.82 | 10.2.10.51     | UDP      | 1292   | 443 → 58427 Len=1250  |
| 22673 | 41.868363 | 10.2.11.211    | 224.0.0.251    | TGMPv2   | 60     | Membership Report group 224.0.0.251                                       |
| 22674 | 41.870828 | 10.2.10.51     | 113.171.237.82 | UDP      | 79     | 58427 → 443 Len=37  |
| 22675 | 41.905611 | 10.2.10.51     | 157.240.199.17 | TCP      | 86     | [TCP Retransmission] 49795 → 443 [PSH, ACK] Seq=33 Ack=467 Min=511 Len=32 |
| 22676 | 41.910895 | 10.2.10.51     | 31.13.77.17    | TCP      | 86     | [TCP Retransmission] 49892 → 443 [PSH, ACK] Seq=33 Ack=29 Min=515 Len=32  |
| 22677 | 41.950917 | 10.2.10.51     | 31.13.77.1     | TCP      | 83     | [TCP Retransmission] 49886 → 443 [PSH, ACK] Seq=59 Ack=51 Min=512 Len=29  |
| 22678 | 41.960871 | 10.2.10.51     | 31.13.77.17    | TCP      | 86     | [TCP Retransmission] 49885 → 443 [PSH, ACK] Seq=33 Ack=29 Min=511 Len=32  |

```
> Frame 1: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bytes) on interface \Device\NPF{...}
> Ethernet II, Src: RouterBo_de:6f:ef (4c:5e:0c:de:6f:ef), Dst: IntelCor_43:92:bb (10:02:b5:43:92:bb)
> Internet Protocol Version 4, Src: 113.171.237.82, Dst: 10.2.10.51
> User Datagram Protocol, Src Port: 443, Dst Port: 58427
Data (1250 bytes)
```

- ▼ Internet Protocol Version 4, Src: 113.171.237.82, Dst: 10.2.10.51
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 1278
  - Identification: 0x01bc (444)
  - ▼ 000. .... = Flags: 0x0
    - 0... .... = Reserved bit: Not set
    - .0.. .... = Don't fragment: Not set
    - ..0. .... = More fragments: Not set
    - ...0 0000 0000 0000 = Fragment Offset: 0
  - Time to Live: 123
  - Protocol: UDP (17)
  - Header Checksum: 0xc600 [validation disabled]
  - [Header checksum status: Unverified]
  - Source Address: 113.171.237.82
  - Destination Address: 10.2.10.51
  - > User Datagram Protocol. Src Port: 443. Dst Port: 58427
- ▼ User Datagram Protocol, Src Port: 443, Dst Port: 58427
  - Source Port: 443
  - Destination Port: 58427
  - Length: 1258
  - Checksum: 0x28af [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 0]
  - > [Timestamps]
  - UDP payload (1250 bytes)
  - ▼ Data (1250 bytes)
    - Data: 59bc94c69a59a84cc1d74eaf2f3f47f5ab994ab9b004a7aafceddd3634a5d6f4edcce923...
    - [Length: 1250]

## 5 (wireshark) filter : get method

http.request.method==GET

| No.   | Time      | Source     | Destination    | Protocol | Length | Info  |
|-------|-----------|------------|----------------|----------|--------|---|
| 37908 | 84.968477 | 10.2.10.51 | 104.71.165.197 | HTTP     | 267    | GET /en-US/livetile/preinstall?region=VN&appid=C98EA580842DBB94058BF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1\r\n |

> Frame 37908: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface \Device\NPF\_{611CB354-C2A7-4D3A-8907-E880CAC7DC67}, id 0

> Ethernet II, Src: IntelCor\_43:92:bb (10:82:b5:43:92:bb), Dst: Routerbo\_de:6f:ef (4c:5e:0c:de:6f:ef)

> Internet Protocol Version 4, Src: 10.2.10.51, Dst: 104.71.165.197

> Transmission Control Protocol, Src Port: 50232, Dst Port: 80, Seq: 1, Ack: 1, Len: 213

▼ Hypertext Transfer Protocol

> GET /en-US/livetile/preinstall?region=VN&appid=C98EA580842DBB94058BF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1\r\n

Connection: Keep-Alive\r\n

User-Agent: Microsoft-WNS/10.0\r\n

Host: tile-service.weather.microsoft.com\r\n

\r\n

[Full request URI: http://tile-service.weather.microsoft.com/en-US/livetile/preinstall?region=VN&appid=C98EA580842DBB94058BF071E1DA76512D21FE36&FORM=Threshold]

[HTTP request 1/1]

## 6 (wireshark) analyze get method in detail

http.request.method==GET

Packet list Narrow & Wide Case sensitive Display filter

| No.   | Time      | Source     | Destination    | Protocol | Length | Info                       |
|-------|-----------|------------|----------------|----------|--------|----------------------------|
| 37908 | 84.968477 | 10.2.10.51 | 104.71.165.197 | HTTP     | 267    | GET /en-US/livetile/preins |

▼ Frame 37908: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface \Device\NPF\_{611CB354-C2A7-4D3A-8907-E880CAC7DC67}

Section number: 1

- > Interface id: 0 (\Device\NPF\_{611CB354-C2A7-4D3A-8907-E880CAC7DC67})
- Encapsulation type: Ethernet (1)
- Arrival Time: Sep 12, 2023 20:39:46.785026000 SE Asia Standard Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1694525986.785026000 seconds
- [Time delta from previous captured frame: 0.000000000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 84.968477000 seconds]
- Frame Number: 37908
- Frame Length: 267 bytes (2136 bits)
- Capture Length: 267 bytes (2136 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp:http]
- [Coloring Rule Name: HTTP]
- [Coloring Rule String: http || tcp.port == 80 || http2]

I choose frame 37908. There are 267 bytes on wire and being captured.

- The interface id is 0 (\Device\NPF\_{611CB354-C2A7-4D3A-8907-E880CAC7DC67})
- Epoch time: 1694525986.785026000 second
- Frame number is 37908
- Frame Length: 267 bytes (2136 bits)

▼ Ethernet II, Src: IntelCor\_43:92:bb (10:02:b5:43:92:bb), Dst: Routerbo\_de:6f:ef (4c:5e:0c:de:6f:ef)

- > Destination: Routerbo\_de:6f:ef (4c:5e:0c:de:6f:ef)
- > Source: IntelCor\_43:92:bb (10:02:b5:43:92:bb)
- Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 10.2.10.51, Dst: 104.71.165.197

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 253
- Identification: 0xcd91 (52625)
- > 010. .... = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: TCP (6)
- Header Checksum: 0x0a28 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.2.10.51
- Destination Address: 104.71.165.197

Ethernet II, Src: IntelCor\_43:92:bb (10:02:b5:43:92:bb), Dst: Routerbo\_de:6f:ef (4c:5e:0c:de:6f:ef)

Destination: Routerbo\_de:6f:ef (4c:5e:0c:de:6f:ef)

Source: InterCol\_43:92:bb (10:02:b5:43:92:bb)

Type: Ipv4 (0x0800)

- Internet Protocol Version 4
- Source address: 10.2.10.51
- Destination address: 104:71:165:197
- Total Length: 253
- Identification: 0xcd91 (52625)
- Time to Live: 128
- Protocol: TCP (6)
- Header Checksum: 0x0a28 [validation disabled]
- Header checksum status: Unverified

```
▼ Transmission Control Protocol, Src Port: 50232, Dst Port: 80, Seq: 1, Ack: 1, Len: 213
  Source Port: 50232
  Destination Port: 80
  [Stream index: 51]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 213]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 860993368
  [Next Sequence Number: 214 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3626548897
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
  Window: 517
  [Calculated window size: 132352]
  [Window size scaling factor: 256]
  Checksum: 0x3b6a [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
▼ Hypertext Transfer Protocol
  > GET /en-US/livetile/preinstall?region=VN&appid=C98EA5B0842DBB9405B8F071E1DA76512D21FE36&FORM=Threshold HTTP/1.1\r\n
    Connection: Keep-Alive\r\n
    User-Agent: Microsoft-WNS/10.0\r\n
    Host: tile-service.weather.microsoft.com\r\n
    \r\n
    [Full request URI: http://tile-service.weather.microsoft.com/en-US/livetile/preinstall?region=VN&appid=C98EA5B0842DBB9405B8F071E1DA76512D21FE36&FORM=Threshold]
    [HTTP request 1/1]
```

Transmission Control Protocol, Src Port: 50232, Dst Port: 80, Seq: 1, Ack: 1: Len: 123

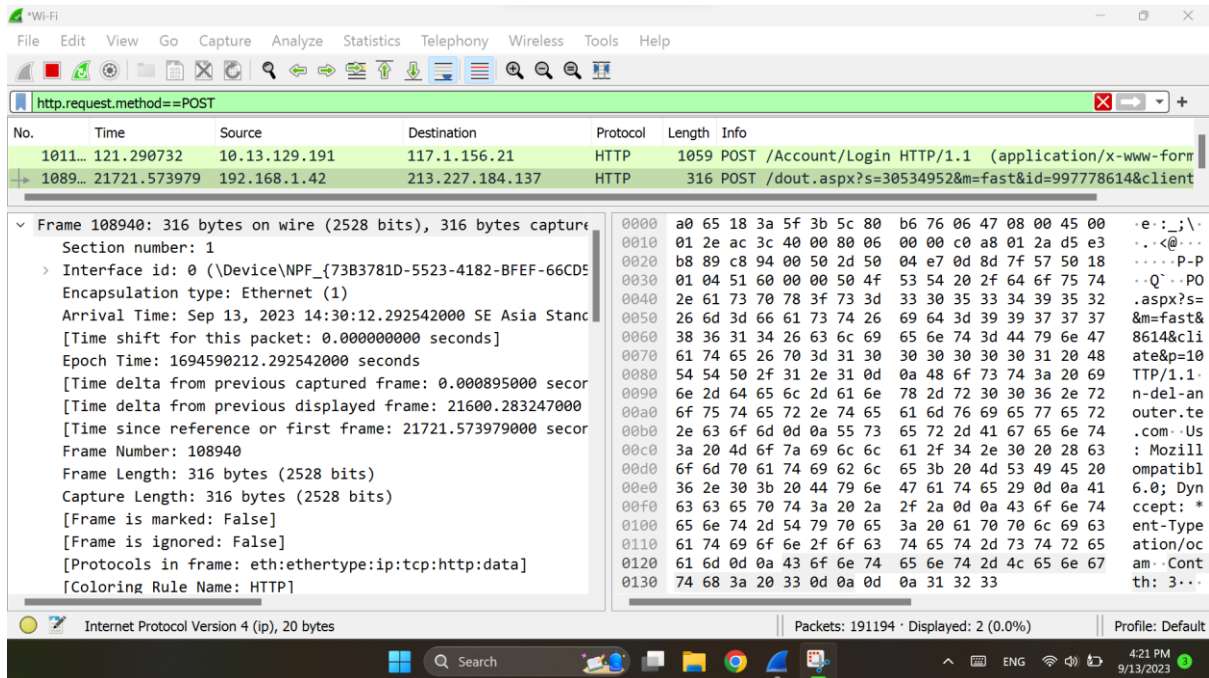
Flags: 0x018 (PSH, ACK)

The HTTP field shows the host and 'full request URI'

## 7 (wireshark) choose one packet

| Apply a display filter ... <Ctrl-/>  |           |                   |                |          |        |   |
|--|-----------|-------------------|----------------|----------|--------|---|
| No.  | Time      | Source            | Destination    | Protocol | Length | Info  |
| 346  | 10.609767 | 10.2.10.51        | 157.240.211.22 | TLSv1.2  | 824    | Application Data  |
| 347  | 10.612575 | 157.240.211.22    | 10.2.10.51     | TCP      | 60     | 443 → 50377 [ACK] Seq=26 Ack=4623 Win=980 Len=0                                   |
| 348  | 10.658768 | 157.240.211.22    | 10.2.10.51     | TCP      | 60     | 443 → 50377 [ACK] Seq=26 Ack=6015 Win=990 Len=0                                   |
| 349  | 10.699095 | 10.2.10.51        | 31.13.75.1     | TLSv1.2  | 115    | Application Data  |
| 350  | 10.701716 | Routerbo_de:6f:ef | Broadcast      | ARP      | 60     | Who has 10.2.10.235? Tell 10.2.10.1   |
| 351  | 10.701998 | 157.240.211.22    | 10.2.10.51     | TLSv1.2  | 96     | [TCP Previous segment not captured], Application Data                             |
| 352  | 10.702938 | 10.2.10.51        | 157.240.211.22 | TCP      | 66     | [TCP Dup ACK 137#1] 50377 → 443 [ACK] Seq=6785 Ack=26 Win=515 Len=0 SLE=53 SRE=95 |
| 353  | 10.704758 | 10.2.10.51        | 31.13.75.1     | TLSv1.2  | 111    | Application Data  |
| 354  | 10.771884 | 31.13.75.1        | 10.2.10.51     | TCP      | 60     | 443 → 50267 [ACK] Seq=399 Ack=128 Win=424 Len=0                                   |
| ▼ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{611CB354-C2A7-4D3A-8907-E880CAC7DC67}, id 0 |           |                   |                |          |        |   |
| ▼ Ethernet II, Src: Routerbo_de:6f:ef (4c:5e:0c:de:6f:ef), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  |           |                   |                |          |        |   |
| ▼ Address Resolution Protocol (request)  |           |                   |                |          |        |   |

## 8 (wireshark) filter : post method



## 9 (wireshark) analyze post method in detail

```
> Frame 108940: 316 bytes on wire (2528 bits), 316 bytes captured on interface 0 (\\Device\\NPF_{73B3781D-5523-4182-BFEF-66CD5})
  Ethernet II, Src: IntelCor_76:06:47 (5c:80:b6:76:06:47), Dst: VnptTech_3a:5f:3b (a0:65:18:3a:5f:3b)
    Destination: VnptTech_3a:5f:3b (a0:65:18:3a:5f:3b)
      Address: VnptTech_3a:5f:3b (a0:65:18:3a:5f:3b)
        .... ..0. .... = LG bit: Globally unique
        .... ..0 .... = IG bit: Individual address
    Source: IntelCor_76:06:47 (5c:80:b6:76:06:47)
      Address: IntelCor_76:06:47 (5c:80:b6:76:06:47)
        .... ..0. .... = LG bit: Globally unique
        .... ..0 .... = IG bit: Individual address
    Type: IPv4 (0x0800)
```

I chose frame 108940: 316 bytes on wire (2528 bits), 316 bytes captured on interface 0 (\\Device\\NPF\_{73B3781D-5523-4182-BFEF-77CD5})

- Interface id: 0 (\\Device\\NPF\_{73B3781D-5523-4182-BFEF-77CD5})
- Epoch Time: 1694590212.292542000 seconds
- Frame Number: 108940
- Frame Length: 316 bytes (2528 bits)



|   |   |
|---|---|
| <pre> &gt; Frame 108940: 316 bytes on wire (2528 bits), 316 bytes captured &gt; Ethernet II, Src: IntelCor_76:06:47 (5c:80:b6:76:06:47), Dst: &gt; Internet Protocol Version 4, Src: 192.168.1.42, Dst: 213.227.2.   0100 .... = Version: 4     .... 0101 = Header Length: 20 bytes (5)   &gt; Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECN)     Total Length: 302     Identification: 0xac3c (44092)   &gt; 010. .... = Flags: 0x2, Don't fragment     .... 0000 0000 0000 = Fragment Offset: 0     Time to Live: 128     Protocol: TCP (6)     Header Checksum: 0x0000 [validation disabled]     [Header checksum status: Unverified]     Source Address: 192.168.1.42     Destination Address: 213.227.184.137   &gt; Transmission Control Protocol, Src Port: 51348, Dst Port: 80, </pre> | <pre> 0000 a0 65 18 3a 5f 3b 5c 80 b6 76 06 47 08 00 45 00 .e.:;.\ 0010 01 2e ac 3c 40 00 80 06 00 00 c0 a8 01 2a d5 e3 ....&lt;@... 0020 b8 89 c8 94 00 50 2d 50 04 e7 0d 8d 7f 57 50 18 .....P-P 0030 01 04 51 60 00 00 50 4f 53 54 20 2f 64 6f 75 74 ..Q'..PO 0040 2e 61 73 70 78 3f 73 3d 33 30 35 33 34 39 35 32 .aspx?s= 0050 26 6d 3d 66 61 73 74 26 69 64 3d 39 39 37 37 37 &amp;m=fast&amp; 0060 38 36 31 34 26 63 6c 69 65 6e 74 3d 44 79 6e 47 8614&amp;cli 0070 61 74 65 26 70 3d 31 30 30 30 30 30 31 20 48 ate&amp;p=10 0080 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 69 TTP/1.1 0090 6e 2d 64 65 6c 2d 61 6e 78 2d 72 30 30 36 2e 72 n-del-an 00a0 6f 75 74 65 72 2e 74 65 61 6d 76 69 65 77 65 72 outer.te 00b0 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 .com..Us 00c0 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 63 : Mozill 00d0 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 ompatibl 00e0 36 2e 30 3b 20 44 79 6e 47 61 74 65 29 0d 0a 41 6.0; Dyn 00f0 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 74 ccept: * 0100 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type 0110 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 ation/oc 0120 61 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 am..Cont 0130 74 68 3a 20 33 0d 0a 0d 0a 31 32 33 th: 3... </pre> |
|---|---|

Internet Protocol Version 4, Src: 192.168.1.42, Dst: 213.227.2

- Total Length: 302
- Time to Live: 128
- Protocol: TCP (6)
- Header Checksum: 0x000 [validation disabled]
- [ Header checksum status: Unverified]
- Source Address: 192.168.1.42

|   |   |
|---|---|
| <pre> &gt; Transmission Control Protocol, Src Port: 51348, Dst Port: 80,   Source Port: 51348   Destination Port: 80   [Stream index: 219]   [Conversation completeness: Complete, WITH_DATA (47)]   [TCP Segment Len: 262]   Sequence Number: 1 (relative sequence number)   Sequence Number (raw): 760218855   [Next Sequence Number: 263 (relative sequence number)]   Acknowledgment Number: 1 (relative ack number)   Acknowledgment number (raw): 227376983   0101 .... = Header Length: 20 bytes (5)   &gt; Flags: 0x018 (PSH, ACK)   Window: 260   [Calculated window size: 66560]   [Window size scaling factor: 256]   Checksum: 0x5160 [unverified] </pre> | <pre> 0000 a0 65 18 3a 5f 3b 5c 80 b6 76 06 47 08 00 45 00 .e.:;.\ 0010 01 2e ac 3c 40 00 80 06 00 00 c0 a8 01 2a d5 e3 ....&lt;@... 0020 b8 89 c8 94 00 50 2d 50 04 e7 0d 8d 7f 57 50 18 .....P-P 0030 01 04 51 60 00 00 50 4f 53 54 20 2f 64 6f 75 74 ..Q'..PO 0040 2e 61 73 70 78 3f 73 3d 33 30 35 33 34 39 35 32 .aspx?s= 0050 26 6d 3d 66 61 73 74 26 69 64 3d 39 39 37 37 37 &amp;m=fast&amp; 0060 38 36 31 34 26 63 6c 69 65 6e 74 3d 44 79 6e 47 8614&amp;cli 0070 61 74 65 26 70 3d 31 30 30 30 30 30 31 20 48 ate&amp;p=10 0080 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 69 TTP/1.1 0090 6e 2d 64 65 6c 2d 61 6e 78 2d 72 30 30 36 2e 72 n-del-an 00a0 6f 75 74 65 72 2e 74 65 61 6d 76 69 65 77 65 72 outer.te 00b0 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 .com..Us 00c0 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 63 : Mozill 00d0 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 ompatibl 00e0 36 2e 30 3b 20 44 79 6e 47 61 74 65 29 0d 0a 41 6.0; Dyn 00f0 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 74 ccept: * 0100 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type 0110 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 ation/oc 0120 61 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 am..Cont 0130 74 68 3a 20 33 0d 0a 0d 0a 31 32 33 th: 3... </pre> |
|---|---|

Transmission Control Protocol, Src Port: 51348, Dst Port: 80

- Source Port: 51348
- Distination Port: 80
- [Stream index: 219]
- [TCP Segment Len: 262]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 760218855
- [Next Sequence Number: 273 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)



- Flags: 0x018 (PSH, ACK)

The image shows a Wireshark packet capture of an HTTP POST request. The left pane displays the packet list and details, while the right pane shows the packet bytes in hexadecimal and ASCII.

**Packet List:**

- Transmission Control Protocol, Src Port: 51348, Dst Port: 80, ...
- Hypertext Transfer Protocol
  - POST /dout.aspx?s=30534952&m=fast&id=997778614&client=DynGate [Expert Info (Chat/Sequence): POST /dout.aspx?s=30534952 ...]

**Details:**

- Request Method: POST
- Request URI: /dout.aspx?s=30534952&m=fast&id=997778614&client=DynGate
- Request Version: HTTP/1.1
- Host: in-del-anx-r006.router.teamviewer.com\r\n
- User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)\r\n
- Accept: \*/\*\r\n
- Content-Type: application/octet-stream\r\n
- Content-Length: 3\r\n
- [Full request URI: <http://in-del-anx-r006.router.teamviewer.com/dout.aspx?s=30534952&m=fast&id=997778614&client=DynGate>]
- [HTTP request 1/1]
- [Response in frame: 108958]
- File Data: 3 bytes

**Packet Bytes:**

|      |   |               |
|------|---|---------------|
| 0000 | a0 65 18 3a 5f 3b 5c 80 b6 76 06 47 08 00 45 00 | e . : _ ; \ . |
| 0010 | 01 2e ac 3c 40 00 80 06 00 00 c0 a8 01 2a d5 e3 | .. . < @ ..   |
| 0020 | b8 89 c8 94 00 50 2d 50 04 e7 0d 8d 7f 57 50 18 | .....P-P      |
| 0030 | 01 04 51 60 00 00 50 4f 53 54 20 2f 64 6f 75 74 | ..Q'..PO      |
| 0040 | 2e 61 73 70 78 3f 73 3d 33 30 35 33 34 39 35 32 | .aspx?s=      |
| 0050 | 26 6d 3d 66 61 73 74 26 69 64 3d 39 39 37 37 37 | &m=fast&      |
| 0060 | 38 36 31 34 26 63 6c 69 65 6e 74 3d 44 79 6e 47 | 8614&cli      |
| 0070 | 61 74 65 26 70 3d 31 30 30 30 30 30 31 20 48    | ate&p=10      |
| 0080 | 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 69 | TTP/1.1.      |
| 0090 | 6e 2d 64 65 6c 2d 61 6e 78 2d 72 30 30 36 2e 72 | n-del-an      |
| 00a0 | 6f 75 74 65 72 2e 74 65 61 6d 76 69 65 77 65 72 | outer.te      |
| 00b0 | 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 | .com..Us      |
| 00c0 | 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 63 | : Mozill      |
| 00d0 | 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 | ompatibl      |
| 00e0 | 36 2e 30 3b 20 44 79 6e 47 61 74 65 29 0d 0a 41 | 6.0; Dyn      |
| 00f0 | 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 74 | ccept: *      |
| 0100 | 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 | ent-Type      |
| 0110 | 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 | ation/oc      |
| 0120 | 61 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 | am..Cont      |
| 0130 | 74 68 3a 20 33 0d 0a 0d 0a 31 32 33             | th: 3...      |

Internet Protocol Version 4 (ip), 20 bytes | Packets: 203071 · Displayed: 4 (0.0%) | Profile: Default

The HTTP field shows some information about POST method like User-Agent, Encoding, Postman-Token, Connectopn. More information full request URI, HTTP request 1/1.