

1. 10.02.15

The screenshot shows a Wireshark packet capture window titled "windows 1 [Running]". The main pane displays a list of captured packets. Packet 9, at time 0.051454, is a GET request from source 10.0.2.15 to destination 172.232.19.208. The packet details pane on the right shows the following information:

- Interface id: 0 (\Device\NPF_{6E37E3D6-5A24-463D-B446-07F636F53652})
- Encapsulation type: Ethernet (1)
- Arrival Time: Feb 14, 2021 18:04:56.253348000 Eastern Standard Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1613343896.253348000 seconds
- [Time delta from previous captured frame: 0.000745000 seconds]
- [Time delta from previous displayed frame: 0.000745000 seconds]
- [Time since reference or first frame: 0.051454000 seconds]
- Frame Number: 69
- Frame Length: 497 bytes (3976 bits)

2. TCP, HTTP UDP
3. GET

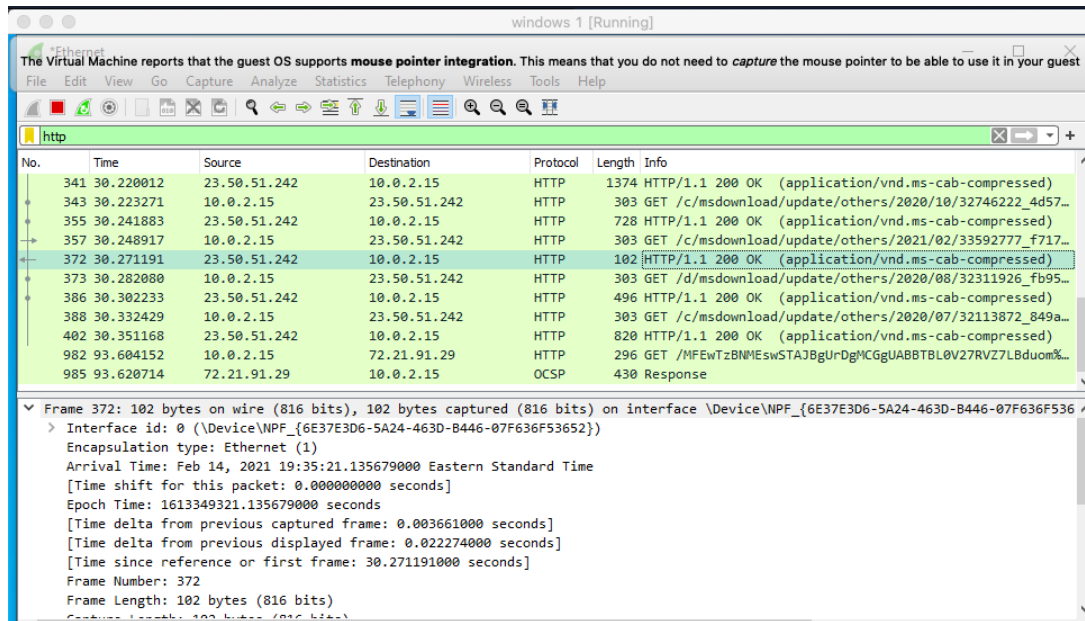
Arrival Time 19:35:07.562777000

The screenshot shows a Wireshark packet capture window titled "windows 1 [Running]". The main pane displays a list of captured packets. Packet 127, at time 16.698289, is a GET request from source 10.0.2.15 to destination 23.50.51.242. The packet details pane on the right shows the following information:

- Interface id: 0 (\Device\NPF_{6E37E3D6-5A24-463D-B446-07F636F53652})
- Encapsulation type: Ethernet (1)
- Arrival Time: Feb 14, 2021 19:35:07.562777000 Eastern Standard Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1613349307.562777000 seconds
- [Time delta from previous captured frame: 0.508929000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 16.698289000 seconds]
- Frame Number: 127
- Frame Length: 303 bytes (2424 bits)

OK

Arrival Time 17:35:21.135679000



The screenshot shows a Wireshark capture of HTTP traffic on an Ethernet interface. The packet list displays several HTTP GET requests and one response. The selected packet (No. 372) is an HTTP 200 OK response from 23.50.51.242 to 10.0.2.15. The packet details pane shows the interface ID, encapsulation type, arrival time, epoch time, and frame number.

No.	Time	Source	Destination	Protocol	Length	Info
341	30.220012	23.50.51.242	10.0.2.15	HTTP	1374	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
343	30.223271	10.0.2.15	23.50.51.242	HTTP	303	GET /c/msdownload/update/others/2020/10/32746222_4d57...
355	30.241883	23.50.51.242	10.0.2.15	HTTP	728	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
357	30.248917	10.0.2.15	23.50.51.242	HTTP	303	GET /c/msdownload/update/others/2021/02/33592777_f717...
372	30.271191	23.50.51.242	10.0.2.15	HTTP	102	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
373	30.282080	10.0.2.15	23.50.51.242	HTTP	303	GET /d/msdownload/update/others/2020/08/32311926_fb95...
386	30.302233	23.50.51.242	10.0.2.15	HTTP	496	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
388	30.332429	10.0.2.15	23.50.51.242	HTTP	303	GET /c/msdownload/update/others/2020/07/32113872_849a...
402	30.351168	23.50.51.242	10.0.2.15	HTTP	820	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
982	93.604152	10.0.2.15	72.21.91.29	HTTP	296	GET /MFewTzBNMEswSTA3BgUrDgMCgUA8BTL0V27RVZ7L8duom%
985	93.620714	72.21.91.29	10.0.2.15	OCSP	430	Response

Frame 372: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{6E37E3D6-5A24-463D-B446-07F636F53652}

Interface id: 0 (\Device\NPF_{6E37E3D6-5A24-463D-B446-07F636F53652})

Encapsulation type: Ethernet (1)

Arrival Time: Feb 14, 2021 19:35:21.135679000 Eastern Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1613349321.135679000 seconds

[Time delta from previous captured frame: 0.003661000 seconds]

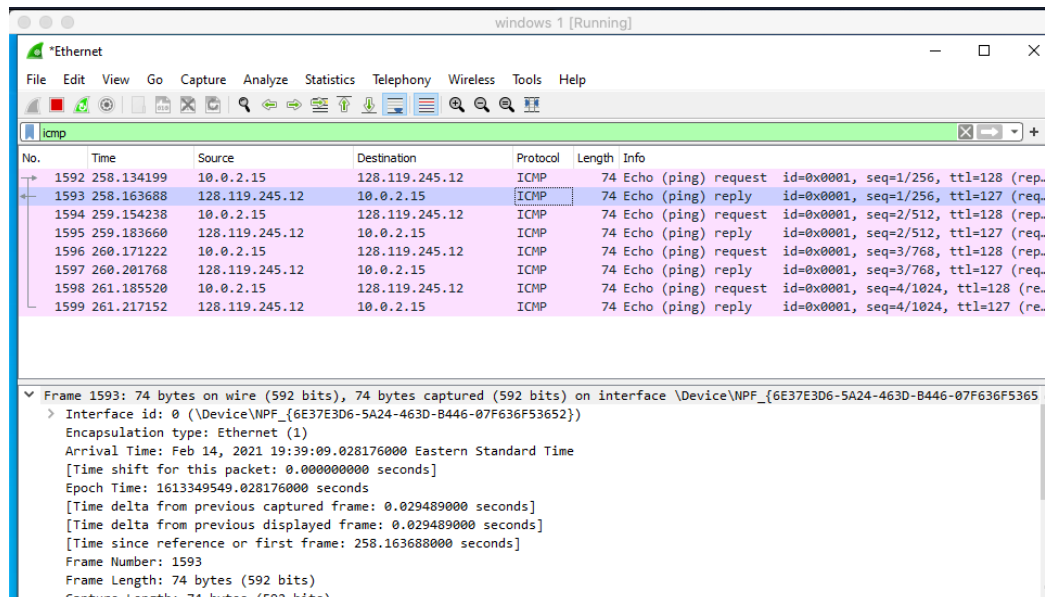
[Time delta from previous displayed frame: 0.022274000 seconds]

[Time since reference or first frame: 30.271191000 seconds]

Frame Number: 372

Frame Length: 102 bytes (816 bits)

4. 128.119.245.12



The screenshot shows a Wireshark capture of ICMP traffic on an Ethernet interface. The packet list displays several Echo (ping) requests and replies between 128.119.245.12 and 10.0.2.15. The selected packet (No. 1593) is an Echo (ping) reply from 128.119.245.12 to 10.0.2.15. The packet details pane shows the interface ID, encapsulation type, arrival time, epoch time, and frame number.

No.	Time	Source	Destination	Protocol	Length	Info
1592	258.134199	10.0.2.15	128.119.245.12	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (rep...
1593	258.163688	128.119.245.12	10.0.2.15	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=127 (req...
1594	259.154238	10.0.2.15	128.119.245.12	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (rep...
1595	259.183660	128.119.245.12	10.0.2.15	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=127 (req...
1596	260.171222	10.0.2.15	128.119.245.12	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (rep...
1597	260.201768	128.119.245.12	10.0.2.15	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=127 (req...
1598	261.185520	10.0.2.15	128.119.245.12	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (re...
1599	261.217152	128.119.245.12	10.0.2.15	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=127 (re...

Frame 1593: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{6E37E3D6-5A24-463D-B446-07F636F53652}

Interface id: 0 (\Device\NPF_{6E37E3D6-5A24-463D-B446-07F636F53652})

Encapsulation type: Ethernet (1)

Arrival Time: Feb 14, 2021 19:39:09.028176000 Eastern Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1613349549.028176000 seconds

[Time delta from previous captured frame: 0.029489000 seconds]

[Time delta from previous displayed frame: 0.029489000 seconds]

[Time since reference or first frame: 258.163688000 seconds]

Frame Number: 1593

Frame Length: 74 bytes (592 bits)

5.GET

```
No.      Time      Source      Destination      Protocol Length Info
127 16.698289 10.0.2.15 23.50.51.242 HTTP 303 GET /c/msdownload/update/others/
2021/02/33633463_9df2082ced9d298f763c4432519fdd5b6d826fc8.cab HTTP/1.1
Frame 127: 303 bytes on wire (2424 bits), 303 bytes captured (2424 bits) on interface \Device\NPF_{6E37E3D6-5A24-463D-B446-07F636F53652}, id 0
  Interface id: 0 (\Device\NPF_{6E37E3D6-5A24-463D-B446-07F636F53652})
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 14, 2021 19:35:07.562777000 Eastern Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1613349307.562777000 seconds
  [Time delta from previous captured frame: 0.508929000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 16.698289000 seconds]
  Frame Number: 127
  Frame Length: 303 bytes (2424 bits)
  Capture Length: 303 bytes (2424 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]
Ethernet II, Src: PcsCompu_65:d8:ed (08:00:27:65:d8:ed), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 23.50.51.242
Transmission Control Protocol, Src Port: 49721, Dst Port: 80, Seq: 1, Ack: 1, Len: 249
  Source Port: 49721
  Destination Port: 80
  [Stream index: 3]
  [TCP Segment Len: 249]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2870123234
  [Next Sequence Number: 250 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 30912002
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window: 64240
  [Calculated window size: 64240]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x5846 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [SEQ/ACK analysis]
  [Timestamps]
  TCP payload (249 bytes)
Hypertext Transfer Protocol
```

OK

No.	Time	Source	Destination	Protocol	Length	Info
127	16.698289	10.0.2.15	23.50.51.242	HTTP	303	GET /c/msdownload/update/others/2021/02/33633463_9df2082ced9d298f763c4432519fdd5b6d826fc8.cab HTTP/1.1

Frame 127: 303 bytes on wire (2424 bits), 303 bytes captured (2424 bits) on interface \Device\NPF_{6E37E3D6-5A24-463D-B446-07F636F53652}, id 0

Interface id: 0 (\Device\NPF_{6E37E3D6-5A24-463D-B446-07F636F53652})

Encapsulation type: Ethernet (1)

Arrival Time: Feb 14, 2021 19:35:07.562777000 Eastern Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1613349307.562777000 seconds

[Time delta from previous captured frame: 0.508929000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 16.698289000 seconds]

Frame Number: 127

Frame Length: 303 bytes (2424 bits)

Capture Length: 303 bytes (2424 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]

Ethernet II, Src: PcsCompu_65:d8:ed (08:00:27:65:d8:ed), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 23.50.51.242

Transmission Control Protocol, Src Port: 49721, Dst Port: 80, Seq: 1, Ack: 1, Len: 249

Source Port: 49721

Destination Port: 80

[Stream index: 3]

[TCP Segment Len: 249]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 2870123234

[Next Sequence Number: 250 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 30912002

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window: 64240

[Calculated window size: 64240]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x5846 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[SEQ/ACK analysis]

[Timestamps]

TCP payload (249 bytes)

Hypertext Transfer Protocol