

65956	1866.694308	192.168.0.167	66.22.219.82	RTCP	102 Sender Report
65957	1867.064790	192.168.0.167	224.0.0.22	IGMPv3	54 Membership Report / Join group 224.0.0.252 for any sources
65958	1867.134788	162.159.130.234	192.168.0.167	TLSv1.2	259 Application Data

```
Wireshark · Packet 1438 · lab1.pcapng
```

> Frame 1438: 671 bytes on wire (5368 bits), 671 bytes captured (5368 bits) on interface \Device\NPF_{44144D08-D1F4-4489-B45D-A581C7D85C84}, id 0

> Ethernet II, Src: WistronI_64:ed:a8 (98:ee:cb:64:ed:a8), Dst: HitronTe_19:32:72 (60:6c:63:19:32:72)

▼ Internet Protocol Version 4, Src: 192.168.0.167, Dst: 128.119.245.12

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 657
- Identification: 0x4585 (17797)
- > 010. = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: TCP (6)
- Header Checksum: 0x0000 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.0.167 ← my computer address
- Destination Address: 128.119.245.12 ← gaia.cs.umass.edu

> Transmission Control Protocol, Src Port: 12044, Dst Port: 80, Seq: 1, Ack: 1, Len: 617

> Hypertext Transfer Protocol

The image displays a Wireshark packet capture window. The top pane shows the packet list, with packet 1438 selected. The middle pane shows the packet details, highlighting the Hypertext Transfer Protocol section. The bottom pane shows the raw packet bytes in hexadecimal and ASCII.

Packet List:

- Frame 1438: 671 bytes on wire (5368 bits), 671 bytes captured (5368 bits) on interface \Device\NPF_{44144D08-D1F4-4489-B45D-A581C7D85C84}, id 0
- Ethernet II, Src: WistronI_64:ed:a8 (98:ee:cb:64:ed:a8), Dst: HitronTe_19:32:72 (60:6c:63:19:32:72)
- Internet Protocol Version 4, Src: 192.168.0.167, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 12044, Dst Port: 80, Seq: 1, Ack: 1, Len: 617

Packet Details:

- Hypertext Transfer Protocol**
 - GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1**
 - [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1]
 - [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Method: GET
 - Request URI: /wireshark-labs/INTRO-wireshark-file1.html
 - Request Version: HTTP/1.1
 - Host: gaia.cs.umass.edu
 - Connection: keep-alive
 - Cache-Control: max-age=0
 - Upgrade-Insecure-Requests: 1
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
 - Accept-Encoding: gzip, deflate
 - Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6
 - If-None-Match: "51-5ea6b81ac3d38"
 - If-Modified-Since: Fri, 07 Oct 2022 05:59:01 GMT
 - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
 - [HTTP request 1/1]
 - [Response in frame: 1447]

Raw Packet Bytes:

Offset	Hex	ASCII
0030	02 01 39 57 00 00 47 45 54 20 2f 77 69 72 65 73	..9W..GE T /wires
0040	68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d	hark-lab s/INTRO-
0050	77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e	wireshar k-file1.
0060	68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48	html HTTP/1.1..H
0070	6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61	ost: gai a.cs.uma
0080	73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69	ss.edu.. Connecti
0090	6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a	on: keep -alive..
00a0	43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d	Cache-Co ntrol: m

☒ Show packet bytes