Abdullah Alrfeedi Lab #3 IT-520

1) What is the IP address?

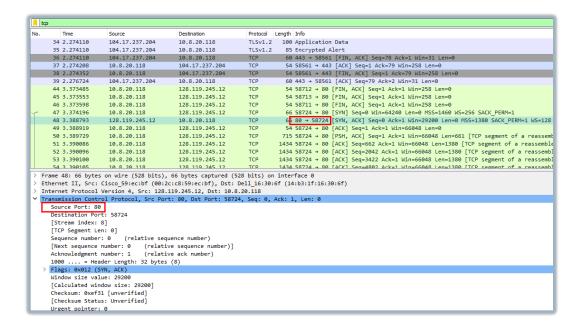
The IP Address is 10.8.20.118

tcp)								
).	Time	Source	Destination	Protocol	Length Info				
	34 2.274110	104.17.237.204	10.8.20.118	TLSv1.2	100 Application Data				
	35 2.274110	104.17.237.204	10.8.20.118	TLSv1.2	85 Encrypted Alert				
	36 2.274110	104.17.237.204	10.8.20.118	TCP	60 443 → 58561 [FIN, ACK] Seq=78 Ack=1 Win=31 Len=0				
	37 2.274208	10.8.20.118	104.17.237.204	TCP	54 58561 → 443 [ACK] Seq=1 Ack=79 Win=258 Len=0				
	38 2.274352	10.8.20.118	104.17.237.204	TCP	54 58561 → 443 [FIN, ACK] Seq=1 Ack=79 Win=258 Len=0				
	39 2.276724	104.17.237.204	10.8.20.118	TCP	60 443 → 58561 [ACK] Seq=79 Ack=2 Win=31 Len=0				
	44 3.373485	10.8.20.118	128.119.245.12	TCP	54 58712 → 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0				
	45 3.373553	10.8.20.118	128.119.245.12	TCP	54 58713 → 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0				
	46 3.373598	10.8.20.118	128.119.245.12	TCP	54 58711 → 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0				
	47 3.374196	10.8.20.118	128.119.245.12	TCP	66 58724 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1				
	48 3.388793	128.119.245.12	10.8.20.118	TCP	66 80 → 58724 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=128				
	49 3.388919	10.8.20.118	128.119.245.12	TCP	54 58724 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0				
	50 3.389729	10.8.20.118	128.119.245.12	TCP	715 58724 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66048 Len=661 [TCP segment of a reassemb				
	51 3.390086	10.8.20.118	128.119.245.12	TCP	1434 58724 → 80 [ACK] Seq=662 Ack=1 Win=66048 Len=1380 [TCP segment of a reassemble				
	52 3.390096	10.8.20.118	128.119.245.12	TCP	1434 58724 → 80 [ACK] Seq=2042 Ack=1 Win=66048 Len=1380 [TCP segment of a reassemb]				
	53 3.390100	10.8.20.118	128.119.245.12	TCP	1434 58724 → 80 [ACK] Seq=3422 Ack=1 Win=66048 Len=1380 [TCP segment of a reassemb]				
	54 3 390105	10 8 20 118	128 119 245 12	TCP	1434 58724 → 80 [ACK] Sen=4802 Ack=1 Win=66048 Len=1380 [TCP segment of a reassemb]				
Fr	ame 48: 66 byte	s on wire (528 bits),	66 bytes captured (5	28 bits) on	interface 0				
Et	hernet II, Src:	Cisco_59:ec:bf (00:2	c:c8:59:ec:bf), Dst:	Dell_16:30:	6f (14:b3:1f:16:30:6f)				
			119.245.12, Dst: 10.8						
Tr	ansmission Cont	rol Protocol, Src Por	t: 80, Dst Port: 5872	4, Seq: 0,	Ack: 1, Len: 0				
	Source Port: 80	9							
	Destination Por	rt: 58724							
	[Stream index:	8]							
[TCP Segment Len: 0]									
	Sequence number	equence number: 0 (relative sequence number)							
	[Next sequence number: 0 (relative sequence number)]								
	Acknowledgment number: 1 (relative ack number)								
	1000 = Header Length: 32 bytes (8)								
>	Flags: 0x012 (SYN, ACK)								
	Window size value: 29200								
	[Calculated window size: 29200]								
	Checksum: 0xef	31 [unverified]							
	[Checksum State	us: Unverified]							
	Urgent pointer:								

2) What is the TCP port number used by your computer to communicate with gaia.cs.umass.edu? The TCP post number used by my computer to communicate with GAIA is 58724.

<u>,</u>	tcp									
No.	Time	Source	Destination	Protocol	Length Info					
	34 2.274110	104.17.237.204	10.8.20.118	TLSv1.2	2 100 Application Data					
	35 2.274110	104.17.237.204	10.8.20.118	TLSv1.2	2 85 Encrypted Alert					
	36 2.274110	104.17.237.204	10.8.20.118	TCP	60 443 → 58561 [FIN, ACK] Seq=78 Ack=1 Win=31 Len=0					
	37 2.274208	10.8.20.118	104.17.237.204	TCP	54 58561 → 443 [ACK] Seq=1 Ack=79 Win=258 Len=0					
	38 2.274352	10.8.20.118	104.17.237.204	TCP	54 58561 → 443 [FIN, ACK] Seq=1 Ack=79 Win=258 Len=0					
	39 2.276724	104.17.237.204	10.8.20.118	TCP	60 443 → 58561 [ACK] Seq=79 Ack=2 Win=31 Len=0					
	44 3.373485	10.8.20.118	128.119.245.12	TCP	54 58712 → 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0					
	45 3.373553	10.8.20.118	128.119.245.12	TCP	54 58713 → 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0					
	46 3.373598	10.8.20.118	128.119.245.12	TCP	54 58711 → 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0					
г	47 3.374196	10.8.20.118	128.119.245.12	TCP	65 58724 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1					
	48 3.388793	128.119.245.12	10.8.20.118	TCP	66 80 → 58724 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=128					
	49 3.388919	10.8.20.118	128.119.245.12	TCP	54 58724 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0					
	50 3.389729	10.8.20.118	128.119.245.12	TCP	715 58724 + 80 [PSH, ACK] Seq=1 Ack=1 Win=66048 Len=661 [TCP segment of a reassembled PC					
	51 3.390086	10.8.20.118	128.119.245.12	TCP	1434 58724 + 80 [ACK] Seq=662 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled PDU					
	52 3.390096	10.8.20.118	128.119.245.12	TCP	1434 58724 → 80 [ACK] Seq=2042 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled PDU					
	53 3.390100	10.8.20.118	128.119.245.12	TCP	1434 58724 → 80 [ACK] Seq=3422 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled PDL					
_	54 3 390105	10 8 20 118	128 119 245 12	TCP	1434 58724 → 80 [ACK] Sec=4802 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled PDU					
			, 66 bytes captured (5							
		::bf (00:2c:c8:59:ec:bf)								
			8.20.118, Dst: 128.119							
~			rt: 58724, Dst Port: 8	0, Seq: 0,	Len: 0					
	Source Port: 58									
	Destination Por									
	[Stream index:									
	[TCP Segment Len: 0]									
	Sequence number: 0 (relative sequence number)									
	[Next sequence number: 0 (relative sequence number)]									
	Acknowledgment number: 0									
	1000 = Header Length: 32 bytes (8)									
	> Flags: 0x002 (SYN)									
	Window size value: 64240									
	[Calculated window size: 64240]									
	Checksum: 0x1d77 [unverified] [Checksum Status: Unverified]									
	Urgent nointer:									
	urgent nointer.	и								

3) What is the TCP port number used by gaia.cs.umass.edu to communicate with your computer? The TCP port number used by gaia.cs.umass.edu to communicate with my computer is 80.



4) What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between your computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

The sequence number of the segment used to initiate the TCP connection is 0. There is also a message contains a SYN flag indicating that it is a SYN segment.

tcp	p								
No.	Time	Source	Destination	Protocol	Length Info				
	34 2.274110	104.17.237.204	10.8.20.118	TLSv1.2	2 100 Application Data				
	35 2.274110	104.17.237.204	10.8.20.118	TLSv1.2	2 85 Encrypted Alert				
	36 2.274110	104.17.237.204	10.8.20.118	TCP	60 443 → 58561 [FIN, ACK] Seq=78 Ack=1 Win=31 Len=0				
	37 2.274208	10.8.20.118	104.17.237.204	TCP	54 58561 → 443 [ACK] Seq=1 Ack=79 Win=258 Len=0				
	38 2.274352	10.8.20.118	104.17.237.204	TCP	54 58561 → 443 [FIN, ACK] Seq=1 Ack=79 Win=258 Len=0				
	39 2.276724	104.17.237.204	10.8.20.118	TCP	60 443 → 58561 [ACK] Seq=79 Ack=2 Win=31 Len=0				
	44 3.373485	10.8.20.118	128.119.245.12	TCP	54 58712 → 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0				
	45 3.373553	10.8.20.118	128.119.245.12	TCP	54 58713 → 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0				
	46 3.373598	10.8.20.118	128.119.245.12	TCP	54 58711 → 80 [FIN, <u>ACK] S</u> eq=1 Ack=1 Win=258 Len=0				
г	47 3.374196	10.8.20.118	128.119.245.12	TCP	66 58724 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1				
	48 3.388793	128.119.245.12	10.8.20.118	TCP	66 80 → 58724 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=128				
	49 3.388919	10.8.20.118	128.119.245.12	TCP	54 58724 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0				
	50 3.389729	10.8.20.118	128.119.245.12	TCP	715 58724 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66048 Len=661 [TCP segment of a reassembled PD				
	51 3.390086	10.8.20.118	128.119.245.12	TCP	1434 58724 → 80 [ACK] Seq=662 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled PDU]				
	52 3.390096	10.8.20.118	128.119.245.12	TCP	1434 58724 → 80 [ACK] Seq=2042 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled PDU				
	53 3.390100	10.8.20.118	128.119.245.12	TCP	1434 58724 → 80 [ACK] Seq=3422 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled PDU				
	54 3 390105	10 8 20 118	128 119 245 12	TCP	1434 58724 → 80 [ACK] Sec=4802 Ack=1 Win=66048 Len=1380 [TCP secment of a reassembled PDU				
> Frame 47: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0									
					::bf (00:2c:c8:59:ec:bf)				
		Version 4, Src: 10.8.							
Y Tr		rol Protocol, Src Port	: 58724, Dst Port: 8	0, Seq: 0,	Len: 0				
Source Port: 58724									
Destination Port: 80									
	[Stream index:								
-	[TCP Segment Le								
L	Sequence number								
[Next sequence number: 0 (relative sequence number)]									
	Acknowledgment								
	1000 = Hea								
- 1		ngs: 0x002 (SYN)							
	Window size va								
	[Calculated window size: 64240]								
	Checksum: 0x1d7								
	[Checksum Statu								
	Urgent nointer	. а							

5) What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? -You must dig deep and find the ACK fromgaia.cs.umass.edu. The sequence number of the SYNACK segment is 0 and the value of the acknowledgement is

Protocol Length Info TLSv1.2 100 Application Data Destination 10.8.20.118 34 2.274110 104.17.237.204 TLSv1.2 85 Encrypted Alert
TCP 66 443 + 58561 [FIN, ACK] Seq=78 Ack=1 Win=31 Lene
TCP 54 58561 + 443 [ACK] Seq=1 Ack=79 Win=258 Lene
TCP 54 58561 + 443 [FIN, ACK] Seq=1 Ack=79 Win=258 Lene 35 2.274110 104.17.237.204 10.8.20.118 10.8.20.118 104.17.237.204 104.17.237.204 36 2.274110 104.17.237.204 38 2.274352 10.8.20.118 54 \$8561 A43 [FIN, ACK] Seq=1 Ack=79 Win=258 Len=0
54 \$8712 - 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0
54 \$8713 - 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0
54 \$8713 - 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0
54 \$8713 - 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0
65 \$8734 - 80 [FIN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
66 \$80 + 58724 [SVI, ACK] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 WS=128
54 \$8724 - 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0 MSS=1380 SACK_PERM=1 WS=128
54 \$8724 - 80 [FSN, ACK] Seq=1 Ack=1 Win=66048 Len=651 [TCP segment of a reassembled 1434 \$8724 - 80 [ACK] Seq=662 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 \$8724 - 80 [ACK] Seq=2642 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 \$8724 - 80 [ACK] Seq=3422 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 \$8724 - 80 [ACK] Seq=3422 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 \$8724 - 80 [ACK] Seq=3422 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 \$8724 - 80 [ACK] Sen=482 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 \$8724 - 80 [ACK] Sen=482 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 \$8724 - 80 [ACK] Sen=482 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 \$8724 - 80 [ACK] Sen=482 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 \$8724 - 80 [ACK] Sen=482 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 \$8724 - 80 [ACK] Sen=482 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 SR724 - 80 [ACK] Sen=482 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 SR724 - 80 [ACK] Sen=482 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 SR724 - 80 [ACK] Sen=482 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 SR724 - 80 [ACK] Sen=482 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 SR724 - 80 [ACK] Sen=482 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 SR724 - 80 [ACK] Sen=482 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled 1434 SR724 - 80 [ACK] S 128.119.245.12 44 3.373485 10.8.20.118 45 3.373553 46 3.373598 47 3.374196 48 3.388793 10.8.20.118 128.119.245.12 128.119.245.12 128.119.245.12 128.119.245.12 10.8.20.118 49 3.388919 10.8.20.118 128.119.245.12 50 3.389729 51 3.390086 52 3.390096 53 3.390100 10.8.20.118 10.8.20.118 10.8.20.118 10.8.20.118 128.119.245.12 128.119.245.12 128.119.245.12 128.119.245.12 10 8 20 118 128 119 245 12 Frame 48: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: (isco_59:ec:bf (00:2c:c6:59:ec:bf), Dst: Dell_16:30:6f (14:b3:1f:16:30:6f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.20.118
Transmission Control Protocol, Src Port: 80, Dst Port: 58724, Seq: 0, Ack: 1, Len: 0 Source Port: 80
Destination Port: 58724
[Stream index: 8]
[TCP Segment Len: 0] [TCP Segment Ler. 0]
Sequence number: 0 (relative sequence number)
Next sequence number: 0 (relative sequence n | Next sequence number: 0 (relative sequence number) |
| Acknowledgment number: 1 (relative ack number) |
| 1800 ... * Header Length: 32 bytes (8) |
| Flags: 0x012 (SYM, ACK) |
| Window size value: 10000 Window size value: 29200 [Calculated window size: 29200] Checksum: 0xef31 [unverified] [Checksum Status: Unverified]

6) What is the sequence number of the TCP segment containing the HTTP POST command? The sequence number of the TCP segment containing the HTTP POST command is 235923.

```
Destination
                                                                                          Length Info
                          Source
                                                                                Protocol
                          10.8.20.118
   278 3.451022
                                                     128.119.245.12
                                                                                            1434 58724 → 80 [ACK] Seq=219363 Ack=1 Win=66048 Len=1380 [TCP
   279 3.451031
                          10.8.20.118
                                                     128.119.245.12
                                                                                            1434 58724 → 80 [ACK] Seq=220743 Ack=1 Win=66048 Len=1380 [TCP
                                                                                TCP
   280 3.451036
                          10.8.20.118
                                                     128.119.245.12
                                                                                            1434 58724 → 80 [ACK]
                                                                                                                       Seq=222123 Ack=1 Win=66048 Len=1380
                                                                                            1434 58724 → 80 [ACK] Seq=223503 Ack=1 Win=66048 Len=1380 [TCP
   281 3.451040
                          10.8.20.118
                                                     128.119.245.12
                                                                                TCP
   282 3.451042
                                                     128.119.245.12
                                                                                            1434 58724 → 80 [ACK] Seq=224883 Ack=1 Win=66048 Len=1380
                                                                                           1434 58724 + 80 [ACK] Seq=226263 Ack=1 Win=66048 Len=1380 [TCP 1434 58724 + 80 [ACK] Seq=227643 Ack=1 Win=66048 Len=1380 [TCP
   283 3.451045
                          10.8.20.118
                                                     128, 119, 245, 12
                                                                                тср
                                                     128.119.245.12
   284 3.451048
                          10.8.20.118
                                                                                ТСР
                                                     128.119.245.12
128.119.245.12
                                                                                           1434 58724 → 80 [PSH, ACK] Seq=229023 Ack=1 Win=66048 Len=1380
1434 58724 → 80 [ACK] Seq=230403 Ack=1 Win=66048 Len=1380 [TCP
   285 3.451050
                          10.8.20.118
                                                                                TCP
   286 3.451053
                          10.8.20.118
                                                                                ТСР
   287 3.451056
                          10.8.20.118
                                                     128,119,245,12
                                                                                           1434 58724 → 80 [ACK] Seq=231783 Ack=1 Win=66048 Len=1380 [TCP 1434 58724 → 80 [ACK] Seq=233163 Ack=1 Win=66048 Len=1380 [TCP
   288 3.451059
                          10.8.20.118
                                                     128.119.245.12
                                                                                ТСР
                                                                                           1434 58724 + 80 [ACK] Seq=234543 Ack=1 Win=66048 Len=1380 [TCP 1434 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (applicat
   289 3.451061
                          10.8.20.118
                                                     128.119.245.12
   290 3.451064
                          10.8.20.118
                                                     128.119.245.12
                                                                                HTTP
                                                                                              60 80 → 58724 [ACK] Seq=1 Ack=136050 Win=240128 Len=0
60 80 → 58724 [ACK] Seq=1 Ack=137430 Win=241152 Len=0
60 80 → 58724 [ACK] Seq=1 Ack=138810 Win=241152 Len=0
   292 3.451102
                          128,119,245,12
                                                     10.8.20.118
                                                                                TCP
   293 3.451128
                          128.119.245.12
                                                     10.8.20.118
   294 3 451796
                         128 119 245 12
                                                     10 8 20 118
                                                                                TCP
                                                                                              60 80 - 58724 [ACK] Sen=1 Ack=142950 Win=241152 Len=0
Frame 290: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface 0
Ethernet II, Src: Dell_16:30:6f (14:b3:1f:16:30:6f), Dst: Cisco_59:ec:bf (00:2c:c8:59:ec:bf)
Internet Protocol Version 4, Src: 10.8.20.118, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58724, Dst Port: 80, Seq: 235923, Ack: 1, Len: 1380
    Source Port: 58724
    Destination Port: 80
    [Stream index: 8]
  Sequence number: 235923
    Sequence number: 235923 (relative sequence number)
[Next sequence number: 237303 (relative sequence number)]
    Acknowledgment number: 1
                                      (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
   Flags: 0x018 (PSH, ACK)
   Window size value: 258
    [Calculated window size: 66048]
   [Window size scaling factor: 256]
Checksum: 0x36e6 [unverified]
   [Checksum Status: Unverified]
```

```
Protocol Length Info
     . Time Source
331 3.467099 128.119.245.12
                                                                              Destination
331 3.467099 128.119.245.12 10.8.20.118 HTTP 831 HTTP/1.1 200 OK (text/html)
Frame 331: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface 0
Ethernet II, Src: Cisco_59:ec:bf (00:2c:c8:59:ec:bf), Dst: Dell_16:30:6f (14:b3:1f:16:30:6f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.20.118
 Transmission Control Protocol, Src Port: 80, Dst Port: 58724, Seq: 1, Ack: 237303, Len: 777
       Source Port: 80
       Destination Port: 58724
      Destination Port: 58724

[Stream index: 8]

[TCP Segment Len: 777]

Sequence number: 1 (relative sequence number)

[Next sequence number: 778 (relative sequence number)]

Acknowledgment number: 237303 (relative ack number)
       0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
       Window size value: 3053
[Calculated window size: 390784]
       [Window size scaling factor: 128]
Checksum: 0x5b9e [unverified]
       [Checksum Status: Unverified]
       Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
       TCP payload (777 bytes)
Hypertext Transfer Protocol
Line-based text data: text/html (11 lines)
```