School of Computer Science and Cybersecurity

CUC

Lab Report #

|  |  |
| --- | --- |
| Lab Name | Wireshark Lab |
| Course Name | Computer Networks |

|  |  |  |  |
| --- | --- | --- | --- |
| Name | 赵婧宇 | Student ID | 201711123028 |

|  |  |
| --- | --- |
| Partners | None |

|  |  |  |  |
| --- | --- | --- | --- |
| Date | 2019-5-21 | Lab Location | CUC #48 |

|  |
| --- |
| Notes： |

**Section I Introduction**

Prepares the reader to understand the whole experiment.

|  |  |
| --- | --- |
| **Must Have:**  1. Clearly stated purpose of the experiment  2. Important background and/or theory | **May include:**  1. Description of specialized equipment  2. Justification of experiment's importance |

The experiment was to learn how to use Wireshark and capture packets using a packet grab tool.

Observing the details of the packets and analyzing them can help us better understand the characteristics of the package.

We need Wireshark-Is a network packet analysis software. The function of network packet analysis software is to capture network packets and display the most detailed network packet data as far as possible. Wireshark USES WinPCAP as an interface to exchange data packets directly with the network card.

**Section II Methods & Materials**

Can be lists or even "refer to lab manual" where appropriate.

**Section III Procedure & Results**

Describes ACTUAL process, especially changes from planned method.

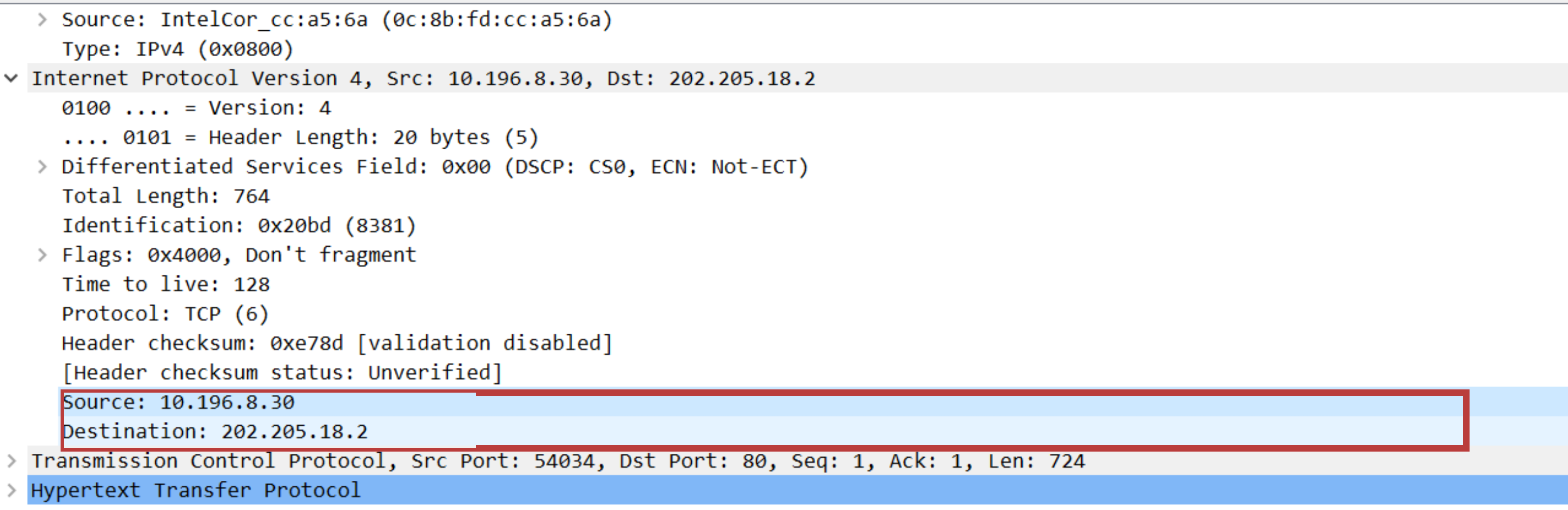
|  |
| --- |
| * **number** and **title** tables and graphs correctly and clearly * draw attention to key points in tables or graphs with a sentence * provide sample calculation only * state key result in sentence form  1. Open the Wireshark and select a interface. 2. Click caputre-> start to grab the packet and open http://eteaching.cuc.edu.cn/computernetworks/Labs/helloworld.html 3. Set up the Filter to “http”. We can see the Packet List Pane, displaying captured packets, active and target addresses, and port number. Packet Details Pane, displaying the fields of the Packet.      1. Here is a Packet Details Pane. This panel is our most important to view each field in the protocol.   Frame: physical layer data Frame overview  Ethernet II: data link layer Ethernet frame header information  Internet Protocol Version 4: Internet layer IP packet header information  Transmission Control Protocol: data segment header information of Transmission layer T, where is TCP  Hypertext Transfer Protocol: information in the application layer, in this case the HTTP Protocol |

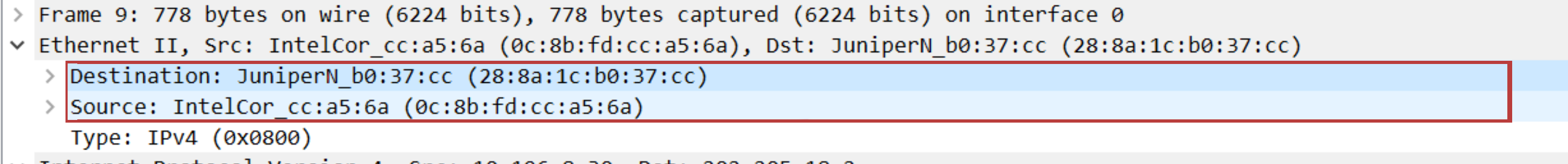
**Section IV Discussion**

Answer the questions in the section [what to hand in] of the lab guide, includes two aspects:

|  |
| --- |
| 1. Analysis = explanation of what can be clearly understood from lab results 2. Interpretation = logical deductions from analysis, explanations of ambiguities. |
| Answer:   1. Different Protocols has different colors, and we can modify these display color rules.      1. HTTP GET |
| HTTP OK |

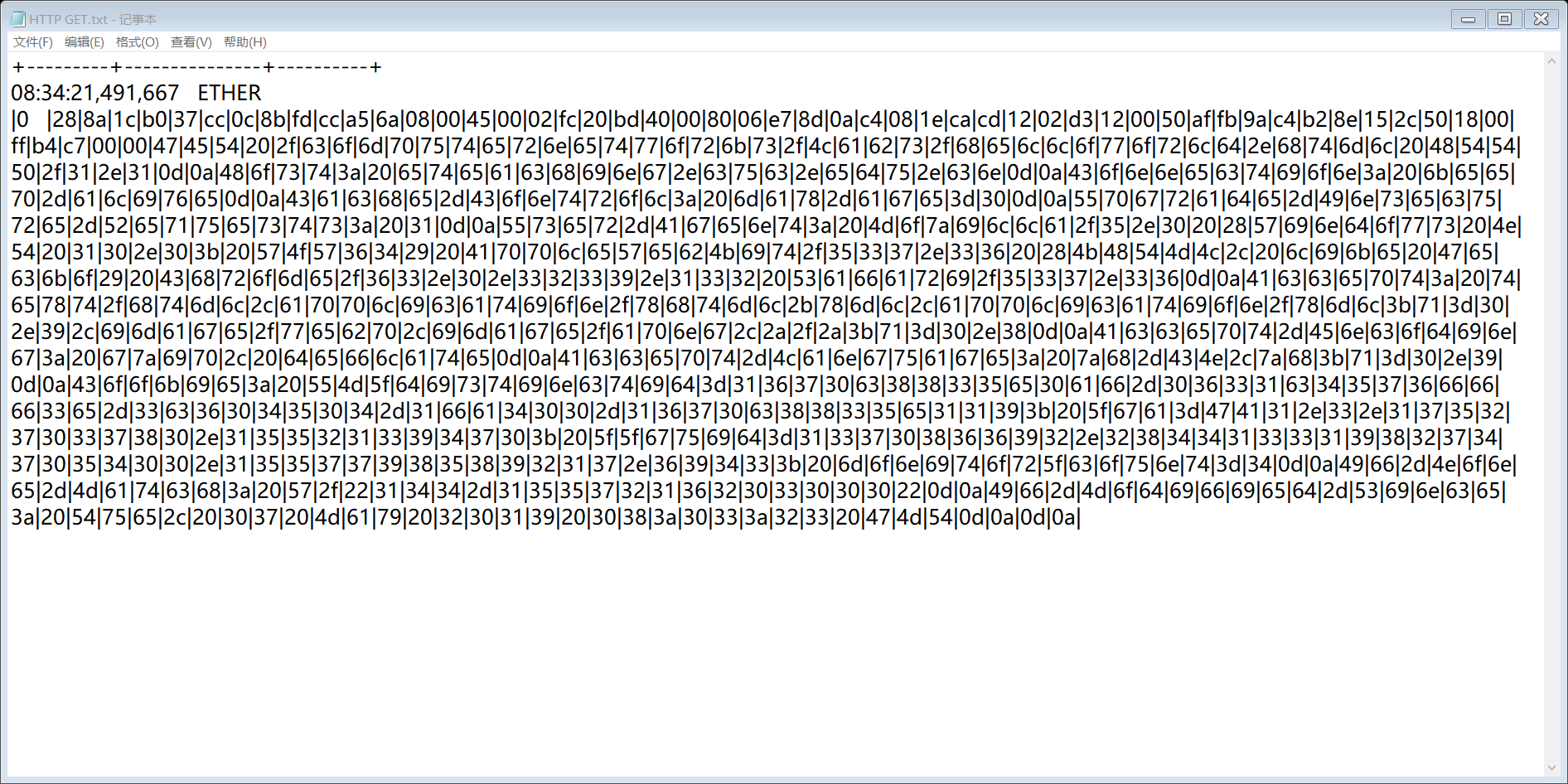
About 21 seconds



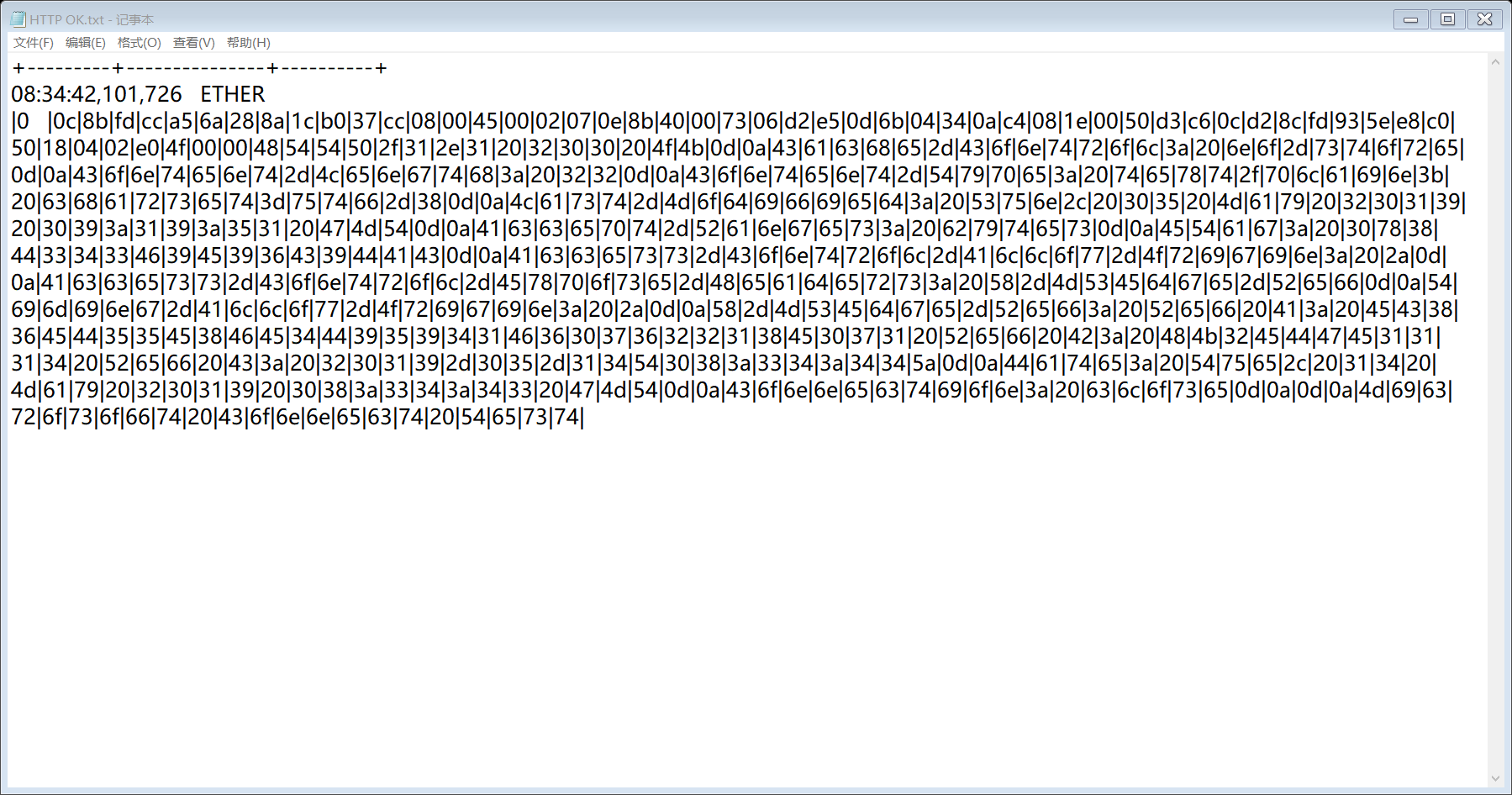
1. 

My computer has Source address and opposite side has Destination address.

1. HTTP GET



HTTP OK



**Section V Conclusion**

States what is known as a result of the experiment.

|  |  |
| --- | --- |
| **Must do:**  1. State what's known  2. Justify that statement | **May do:**  1. State significance of findings  2. Suggest further research |

From this experience, I know how to use Wireshark capture network packets and display the details of network packets. But Wireshark can only view packets, not modify the contents of the packets, or send packets. Each line of packet information corresponds to the OSI seven layer model. Here we need to pay attention to the network layer IP packet header information and the data link layer Ethernet frame header information.