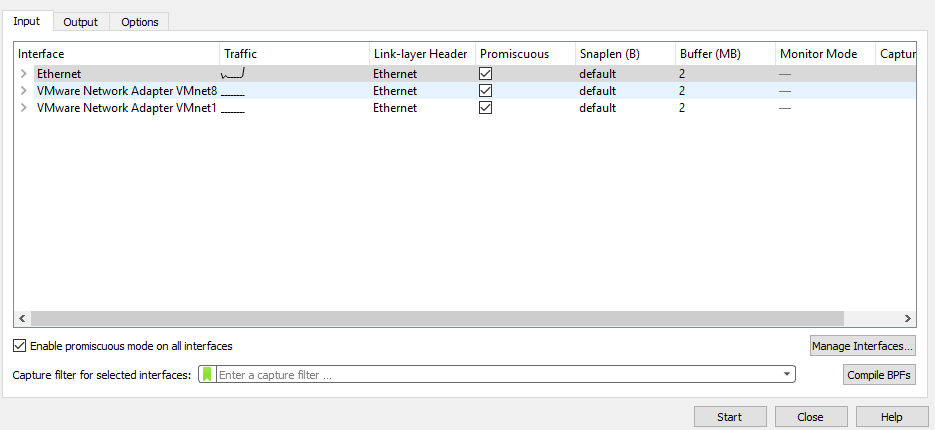
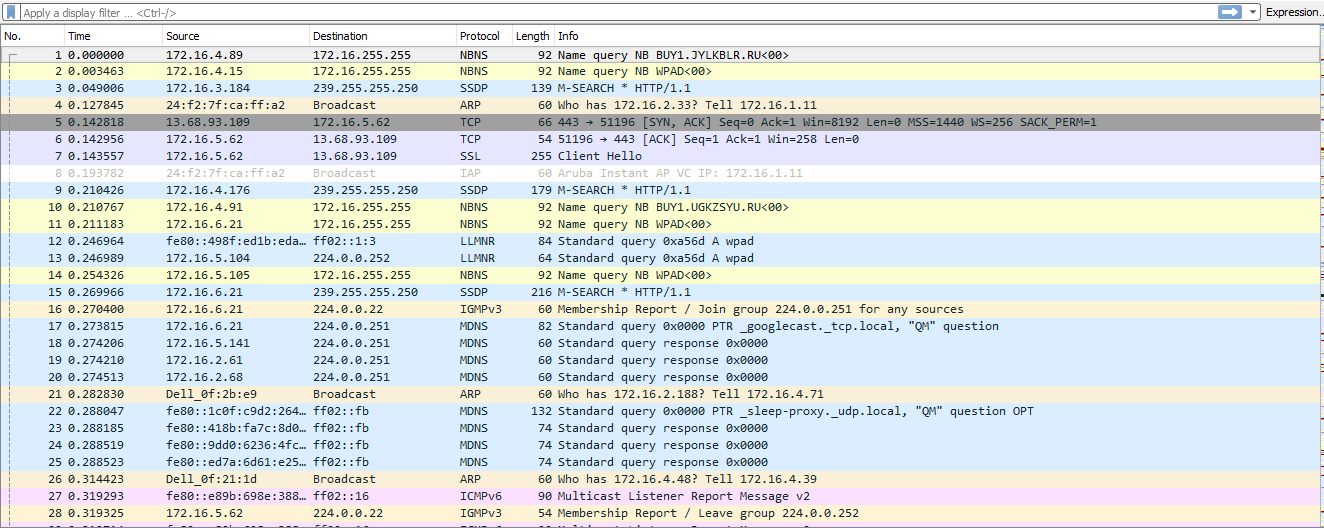
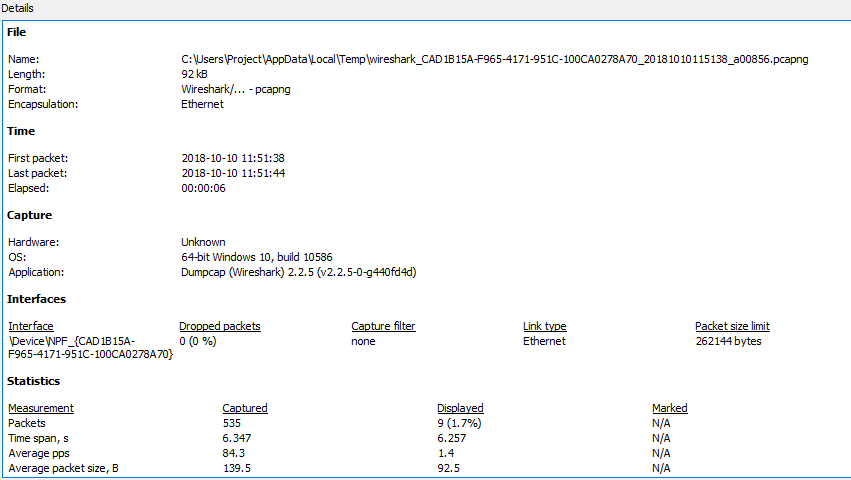
|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Hope Foundation’s,**  **Finolex Academy of Management and Technology, Ratnagiri** | | | | | | | | | |
| **Department of Information Technology** | | | | | | | | | |
| Subject name: SECURITY LAB | | | | | | | | Subject Code: ITL502 | | | |
| Class | | TE IT | | Semester – V (CBCGS) | | | | Academic year: 2018-19 | | | |
| Name of Student | | **Kazi Jawwad A Rahim** | | | | | **QUIZ Score : 06** | | | | |
| Roll No | | **32** | | | Experiment No. | | | | | 07 | |
| Title**. Study of packet sniffer tools wireshark** | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. **Course objectives applicable:**  * To explore the different network reconnaissance tools to gather information about n/ws * To explore and use tools like sniffers, port scanners and other related tools for analyzing   packets in a network. | | | | | | | | | | | |
| 1. **Course outcomes applicable:**  * Explore the different network reconnaissance tools to gather information about networks * Use tools like sniffers, port scanners and other related tools for analyzing packets in network. | | | | | | | | | | | |
| **3. Learning Objectives:**  1. Observer performance in promiscuous as well as non-promiscuous mode.  2. Show the packets can be traced based on different filters. | | | | | | | | | | | |
| **Practical applications of the assignment/experiment:**   * Network administrators use it to troubleshoot network problems * Network security engineers use it to examine security problems * QA engineers use it to verify network applications * Developers use it to debug protocol implementations * People use it to learn network protocol internals | | | | | | | | | | | |
| **Prerequisites**:   * Wireshark can also be downloaded from here: https://www.wireshark.org/download.html | | | | | | | | | | | |
| **6. Hardware Requirements**:   1. PC with 4GB RAM, 500GB HDD.   **7. Software Requirements:**  1. Wireshark tool | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **8. Quiz Questions (if any): (Online Exam will be taken separately batchwise, attach the certificate/ Marks obtained)**   * What is packet sniffer? * How to sniff passwords with wireshark? * List packet sniffing tools other than mentioned above? | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **9. Experiment/Assignment Evaluation:** | | | | | | | | | | | |
| **Sr. No.** | **Parameters** | | | | | | | | **Marks obtained** | | **Out of** |
| **1** | Technical Understanding (Assessment may be done based on Q & A **or** any other relevant method.) Teacher should mention the other method used - | | | | | | | |  | | 6 |
| **2** | Neatness/presentation | | | | | | | |  | | 2 |
| **3** | Punctuality | | | | | | | |  | | 2 |
| **Date of performance (DOP)** | | |  | | | **Total marks obtained** | | |  | | **10** |
| **Date of checking (DOC)** | | |  | | | **Signature of teacher** | | | | | |



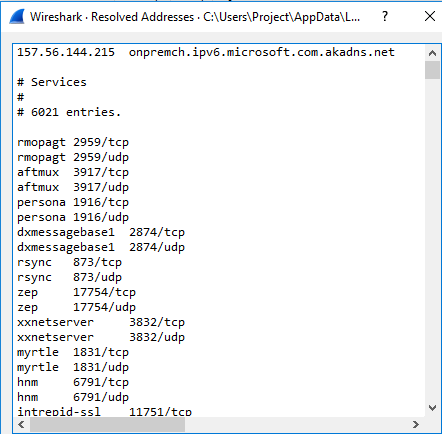


STATISTICS:

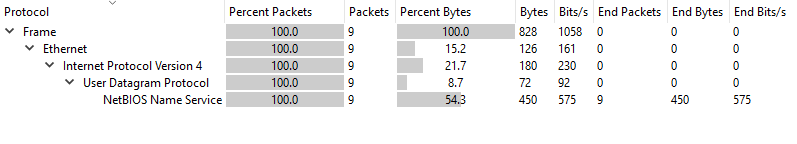
1. **Capture file properties**



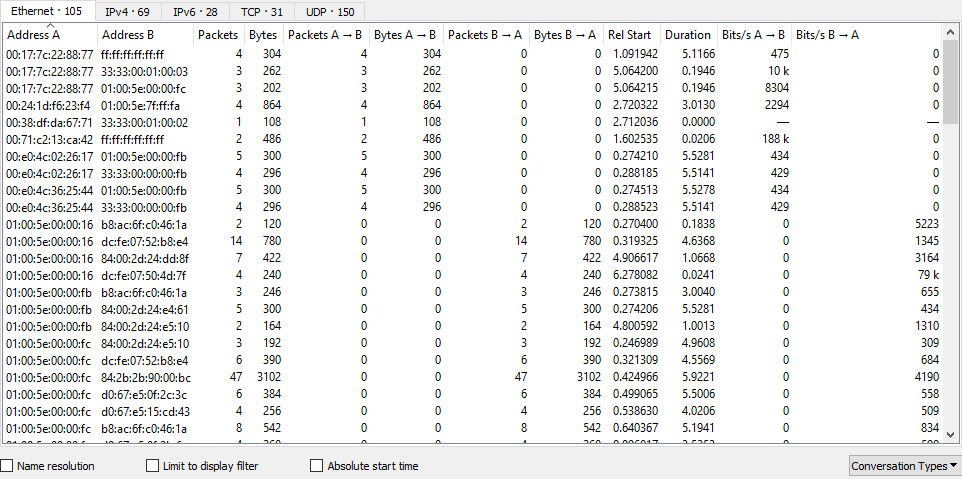
1. **Resolved addresses**



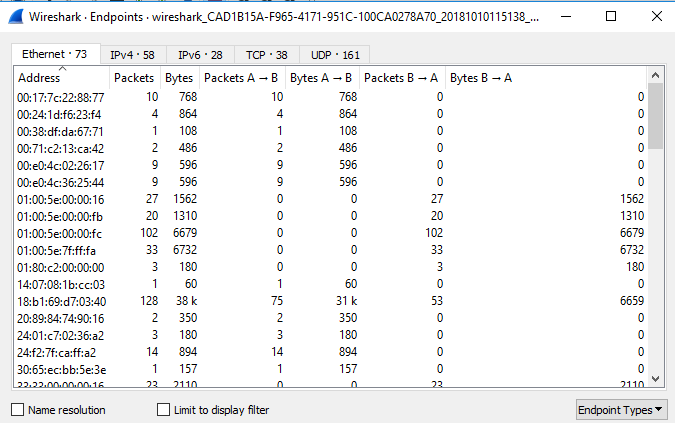
**3)Protocol hierarchy**



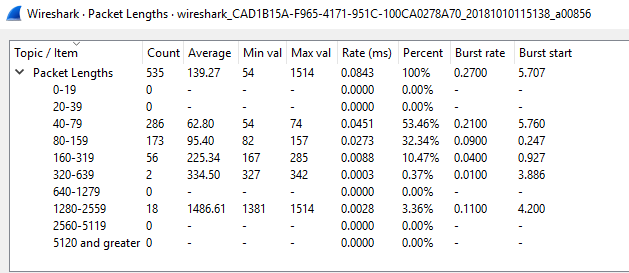
1. **Conversions**



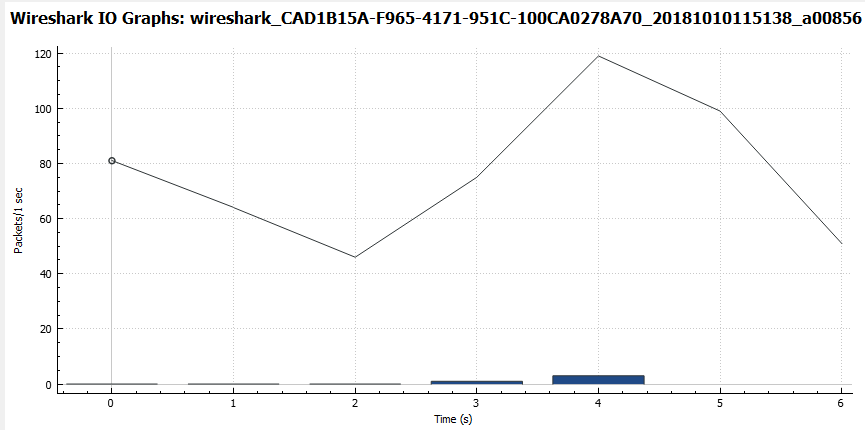
1. **Endpoints**



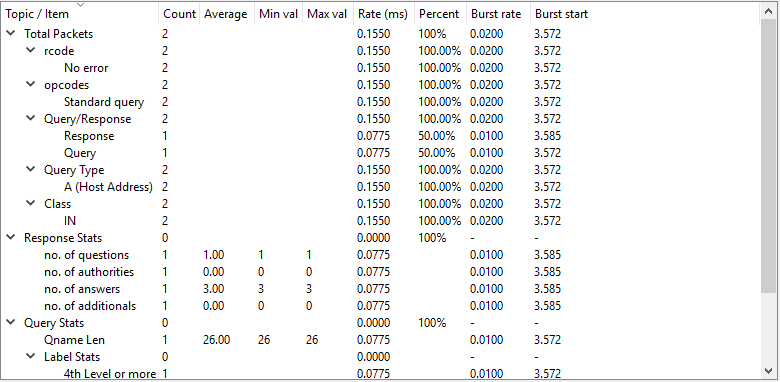
1. **Packet lengths**



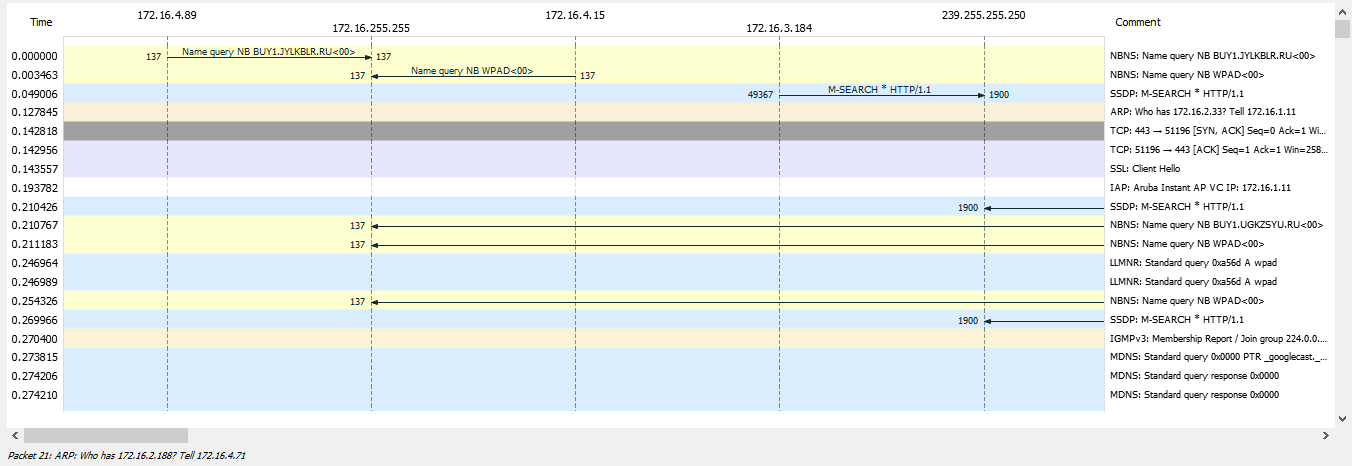
1. **I/O graph**



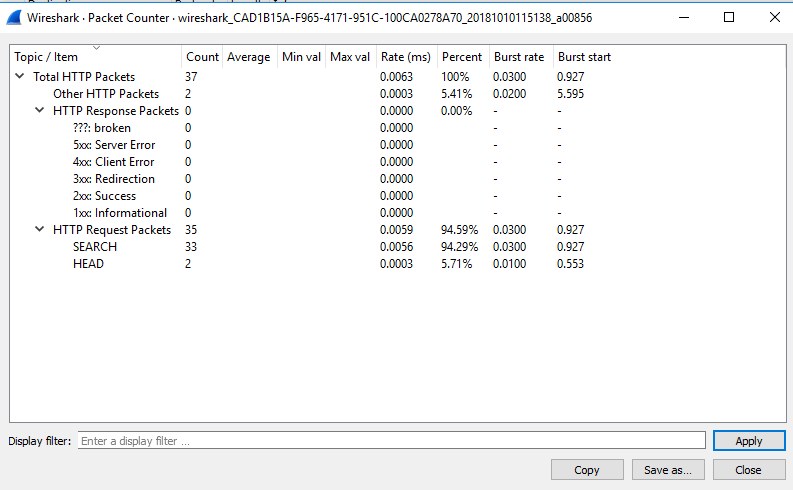
1. **DNS**



1. **Flow graph**

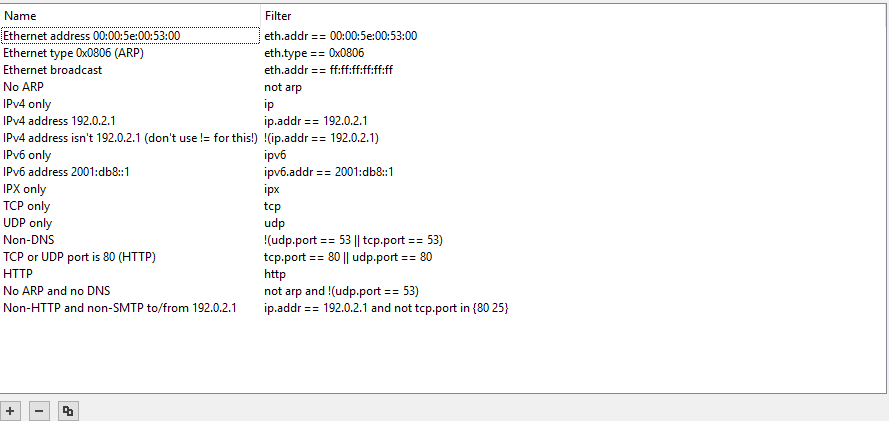


1. **http packet counter**

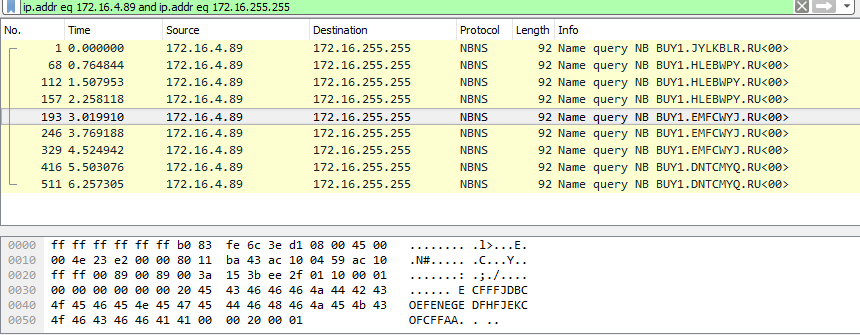


ANALYZE:

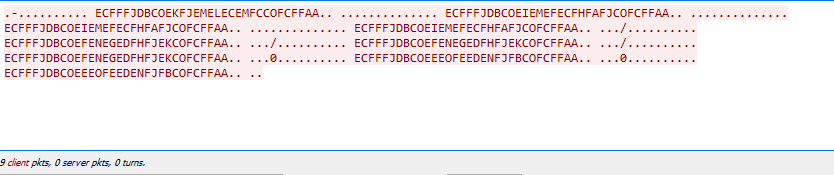
1. **Display filters**



**2)Conversation filter- IPV4**



1. **Follow- UDP stream**



**References** :

* http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm
* https://samsclass.info/120/proj/p3-wireshark.htm
* http://sectools.org/tag/sniffers/