WIRESHARK

Introduction :

Wireshark is a packet sniffing open source software that supports many possible network interfaces the packets can be sniffed from. Along with the packet capturing , it also breaks down the captured packets in the efficient manner (protocol wise) including application layer protocols , transport layer protocols, network layer protocol and data link layer protocols and its details.

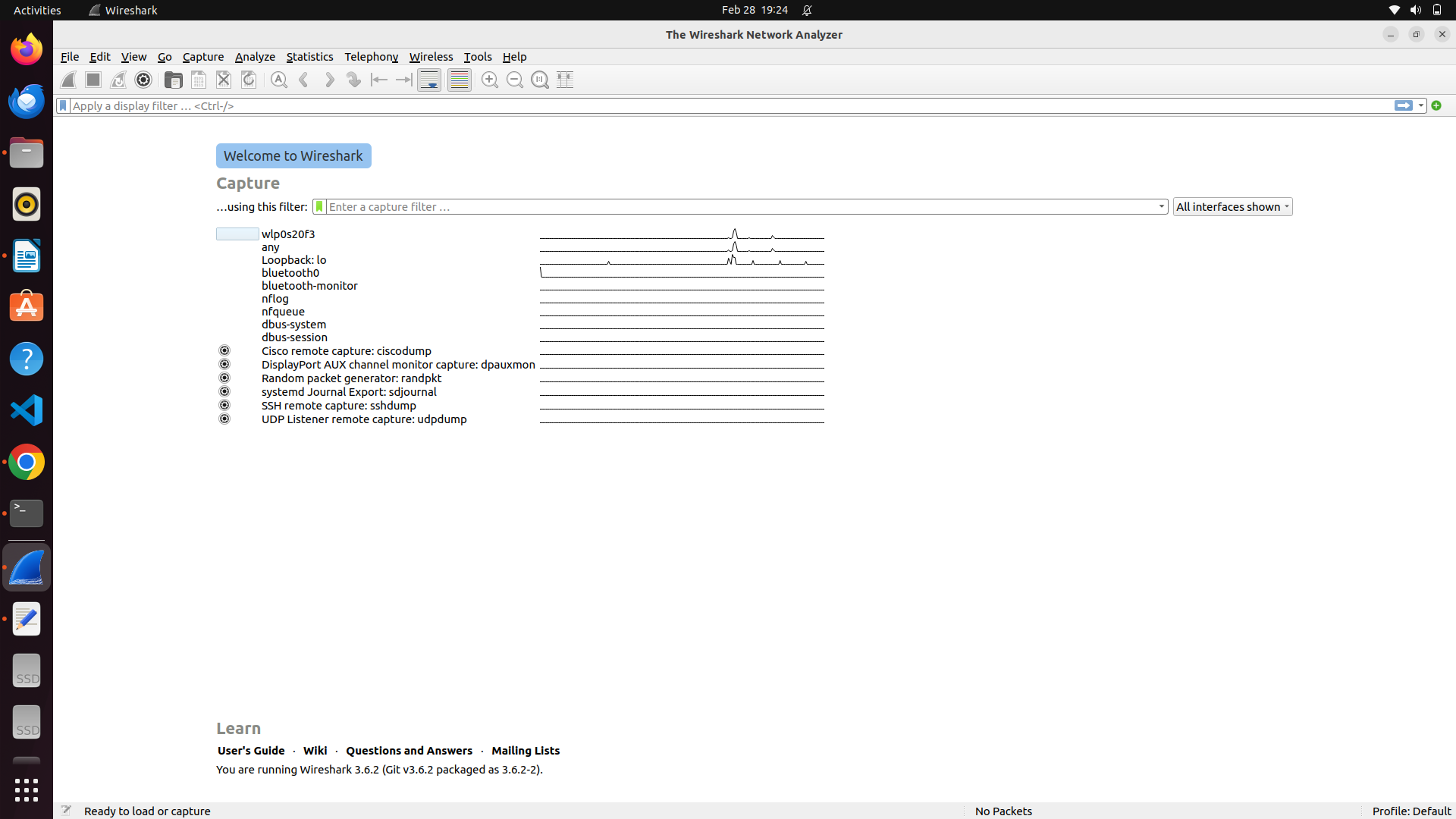
This software can be used by network administrators to troubleshoot network related issues. This can be used by network security engineers to troubleshoot security related issues and can be used by anyone with basic theoretical knowledge on networking to practically understand the internals of the day to day network based data transfer.

In general , any packet will start from application layer with its own protocol like http , https , smtp etc (with unique port) . Application layer (takes care of mail , web based or GUI based data transfer , Remote access of the device etc) payload will be encapsulated with the headers of each and every layers followed by before reaching physical layer (which transmits the bits in the form of signals or wave with respect to the media). Presentation layer generally takes care of encryption , Encoding and compression in Tx side (opposite in Rx side) , Session layer takes care of initiating, maintaining , resuming and terminating the sessions safely either via TLS or SSH protocols with dialogue control , authentication and synchronization checkpoints for efficient session management. Transport Layer takes care of port addressing based on the application , Segmentation , acts as higher level reliability control layer with error control , flow control and connection control protocols .(either TCP or UDP) Network Layer takes care of Logical addressing (IP of the src and dest router interface) and routing process ; acts as a focal point in TCP/IP suite. Data link layer takes care of framing , fragmentation , MAC addressing , Error control , Flow Control and Access control techniques with both headers and trailers attached to the packet. With two sub layers : Logical Link control (LLC) as a upper sub layer which acts as interface to higher level protocols whereas MAC layer as a lower sub layer takes care of NIC , Encoding , Tx and Rx process of frames with Physical layer.

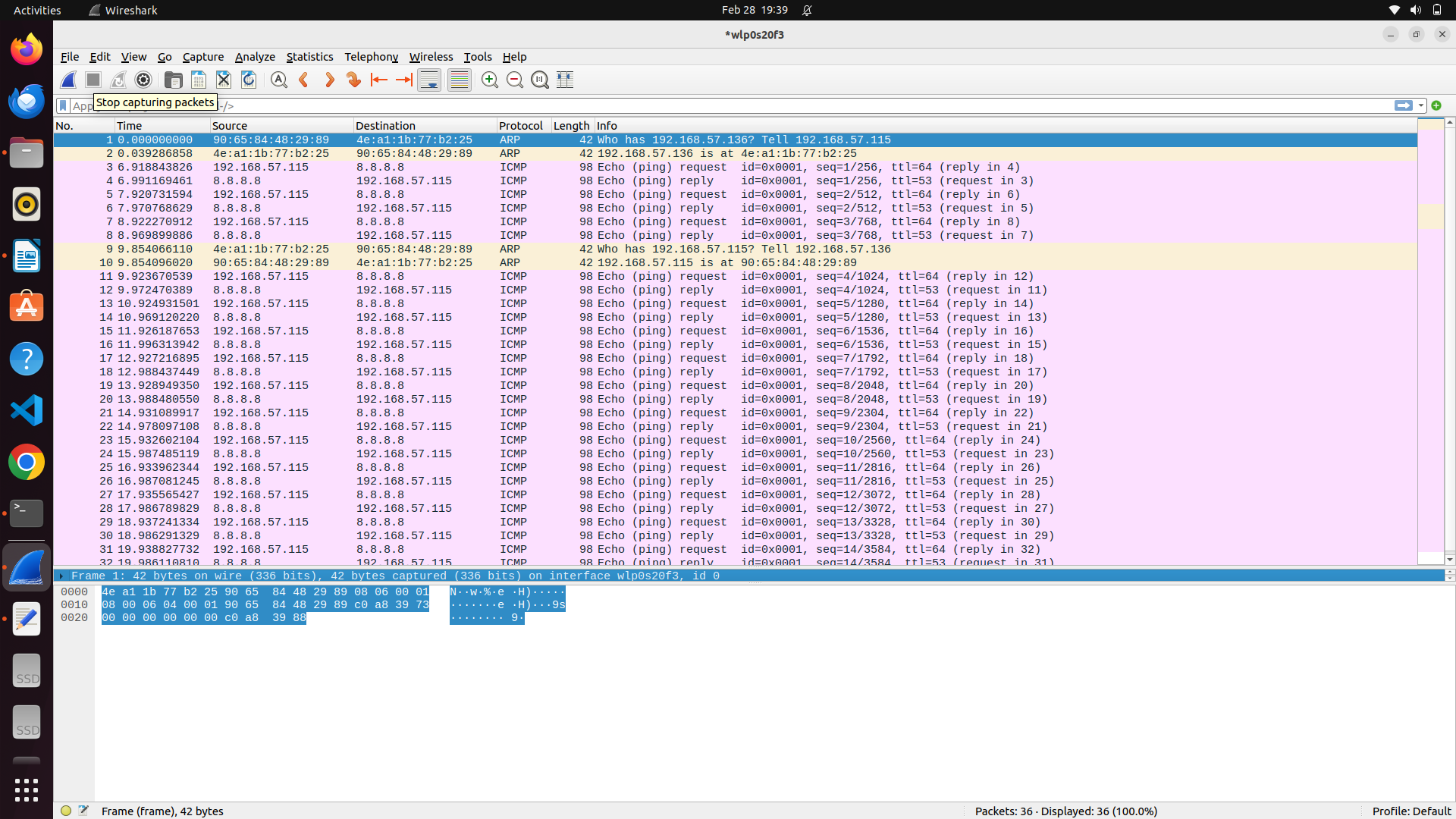
WIRESHARK DEMONSTRATION

1. Wireshark can be opened from Terminal just by typing "wireshark" in prompt or by conventional procedure too.

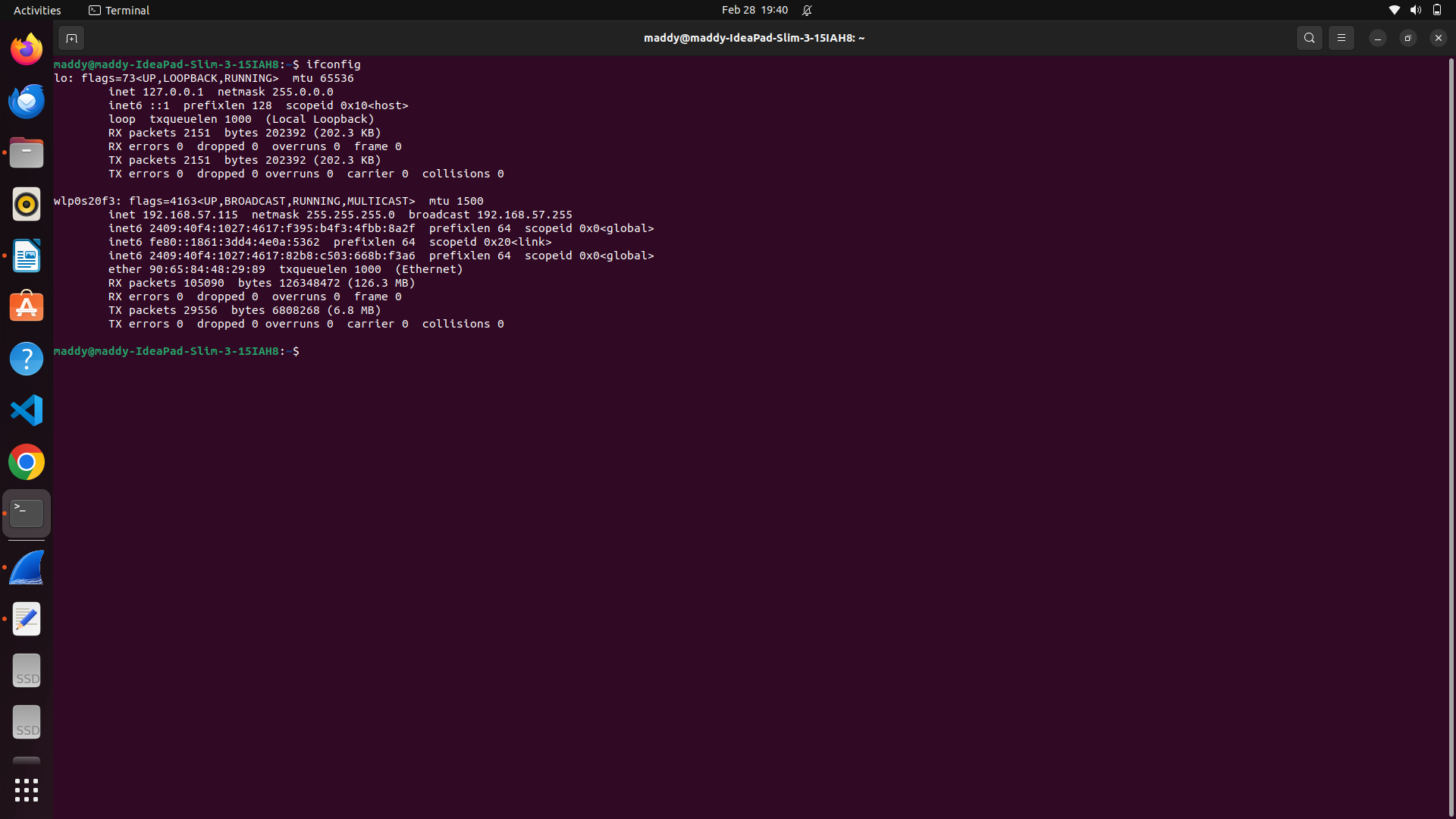
2. Once , wireshark got opened , it is possible to see all the active interfaces from which packets can be sniffed as follows:



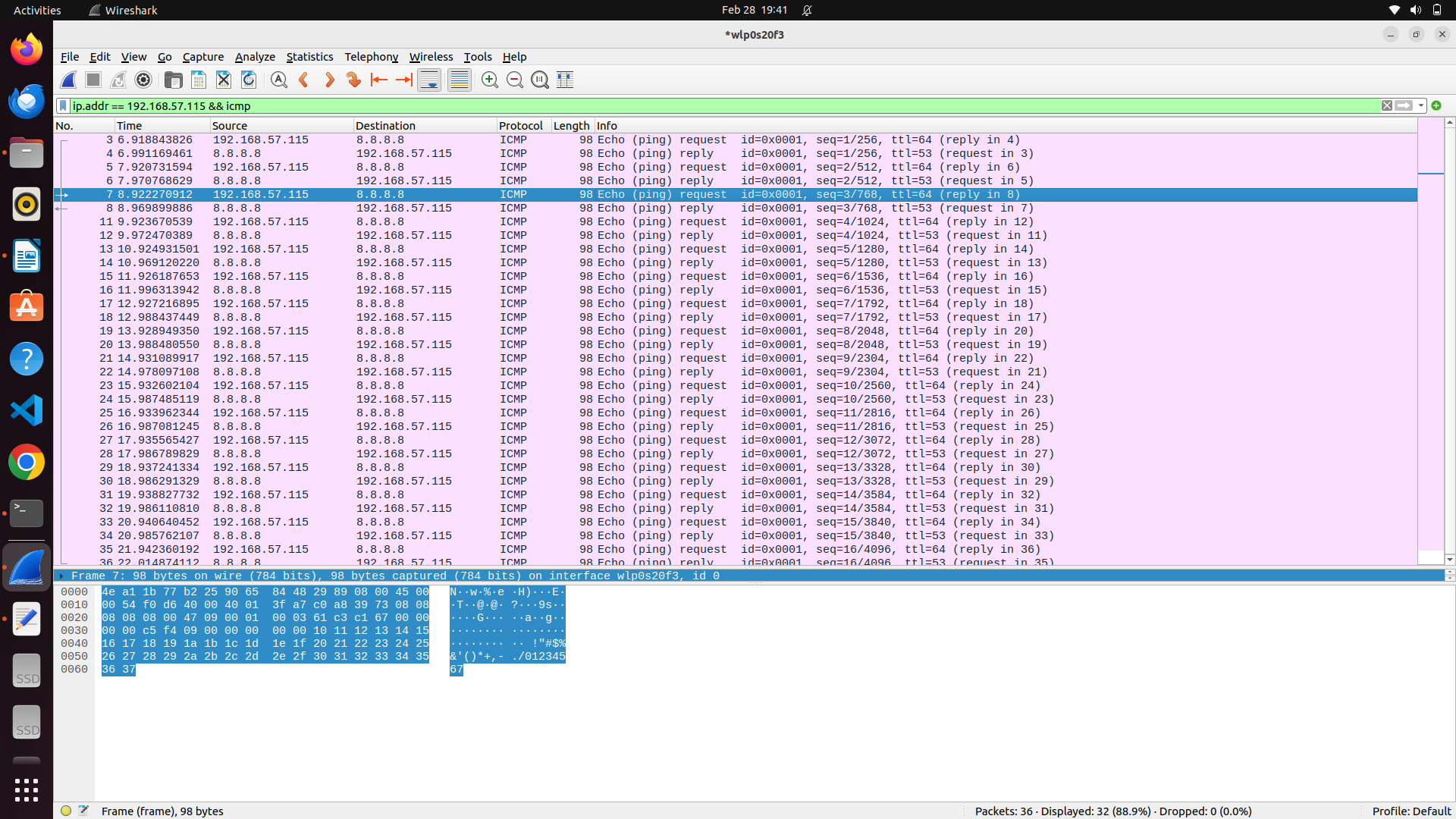
3. Double click on the interface needed and it automatically starts capturing the packets from various possible protocols as shown :



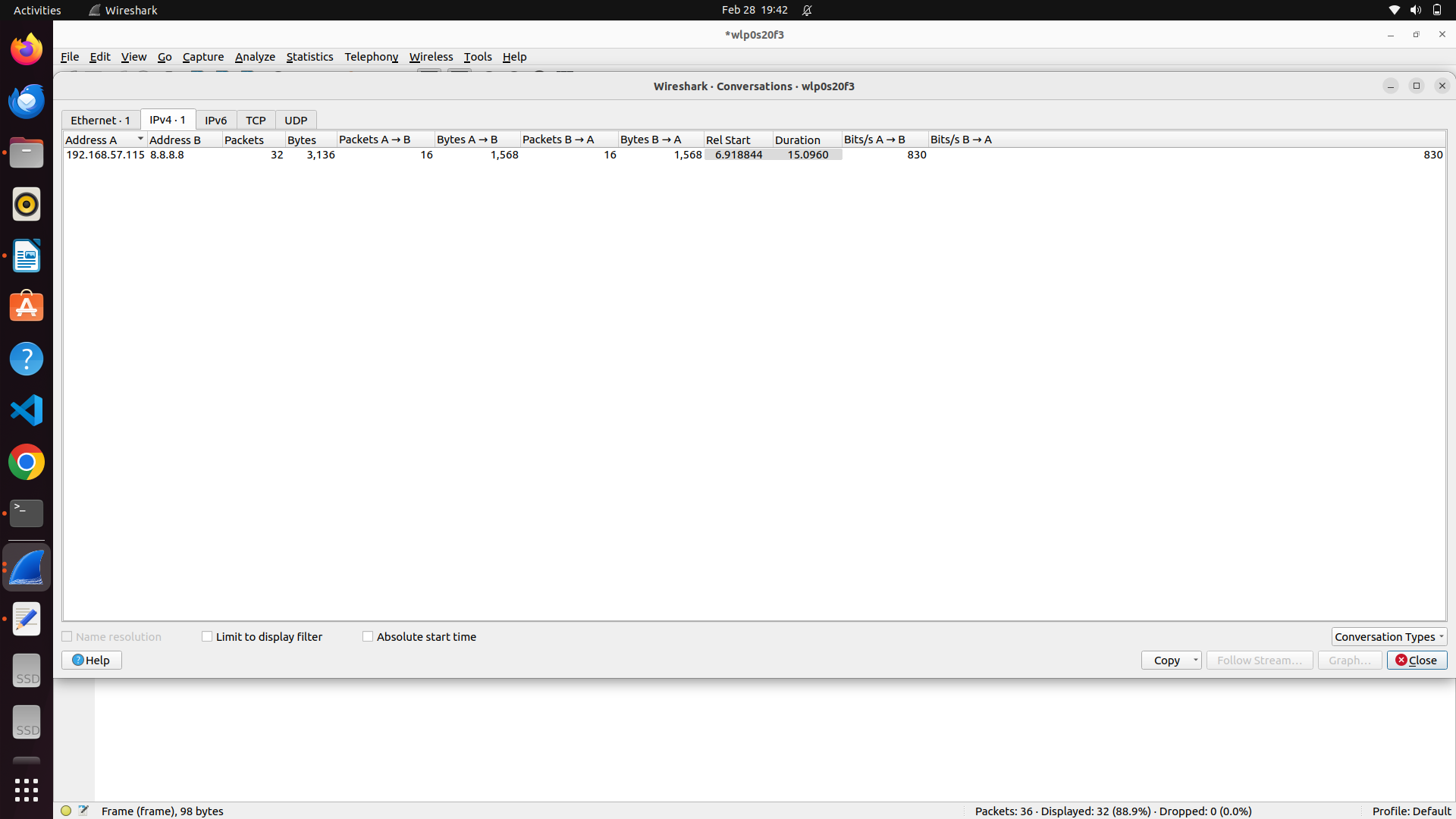
4. To apply filter, especially based on IP address of that current device, use ifconfig on terminal as shown:



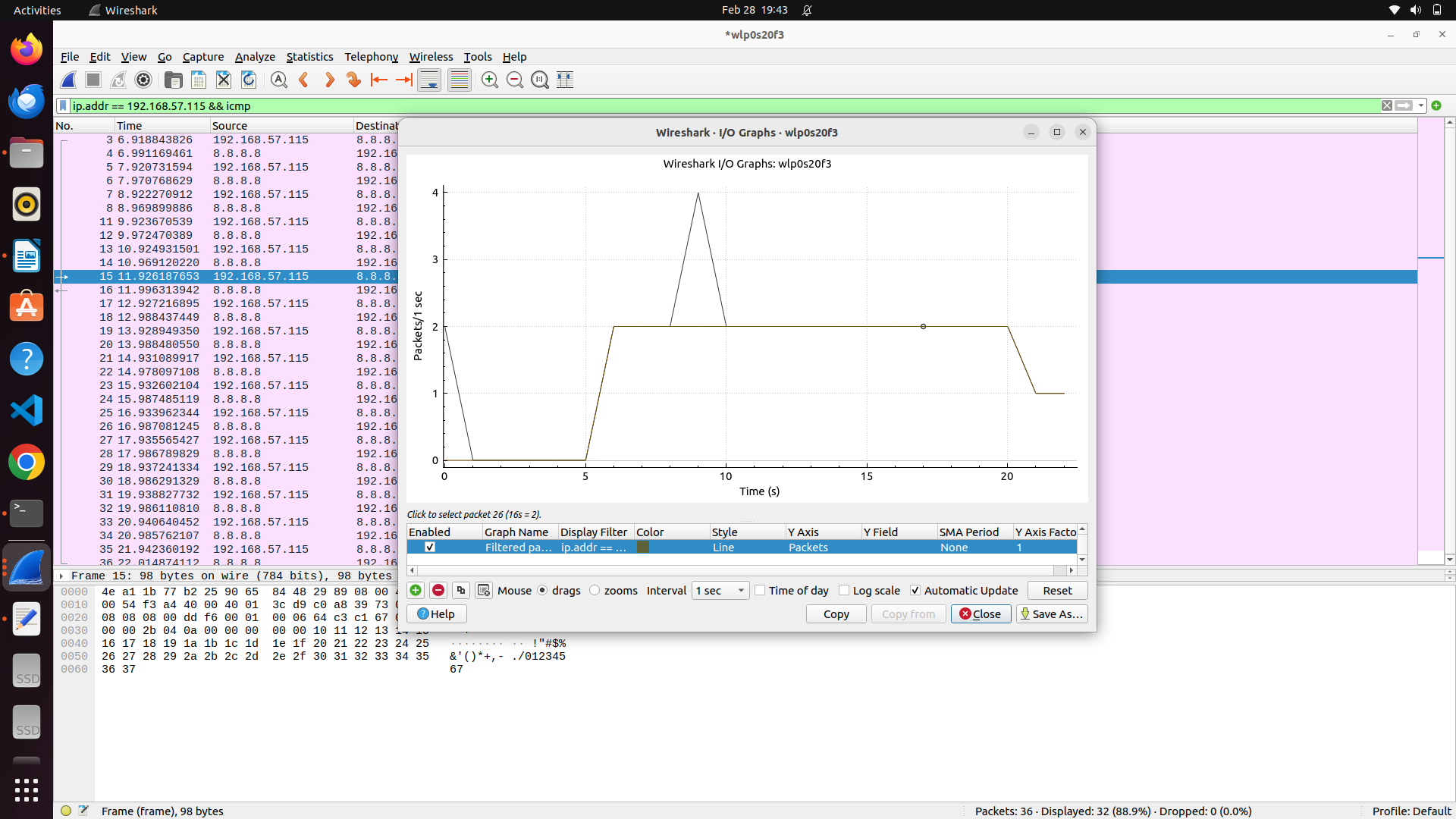
5. Apply filter in the top search box in wireshark as follows. Here, for demonstration, transaction with particular IP as well as involved in Internet Control Message Protocol (commonly used for ping) is shown



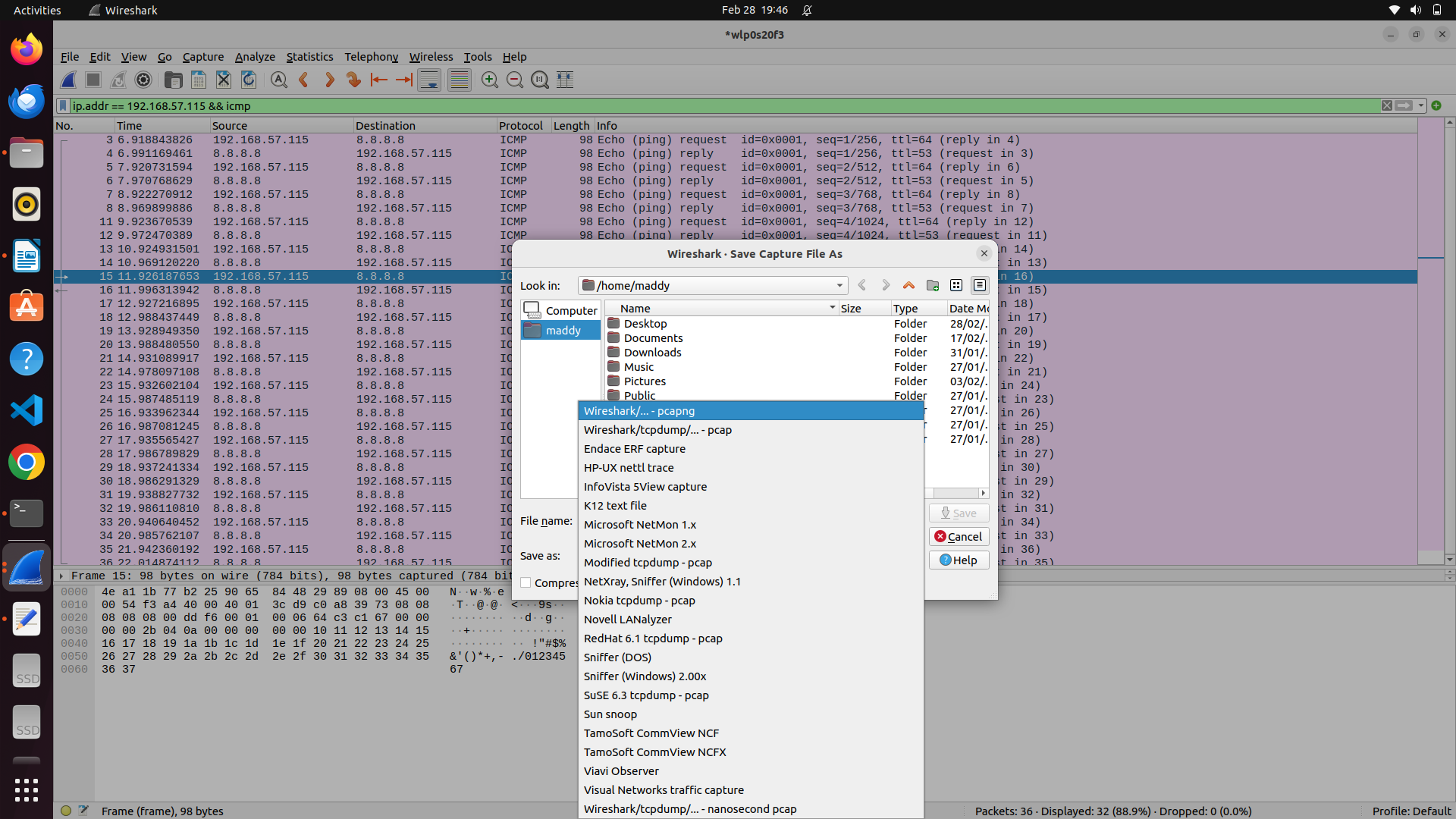
6. Conversation filter can be applied to have concise view and also to track particular protocol like TCP or UDP stream conversation, as shown



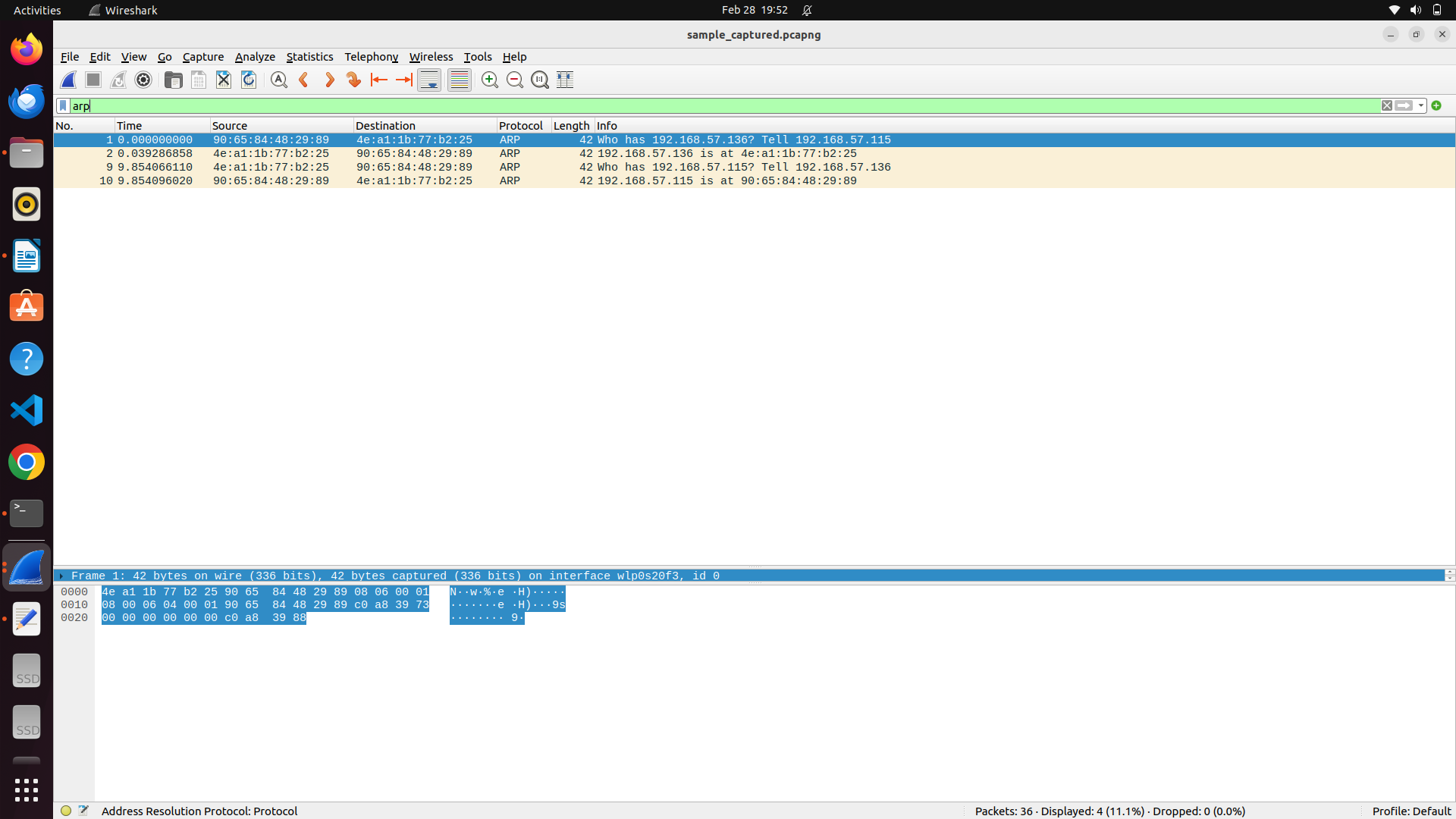
7. In the statistics window, there are many options among which one option is I/O graph which gives the plot of time vs number of packet (traffic) as shown:



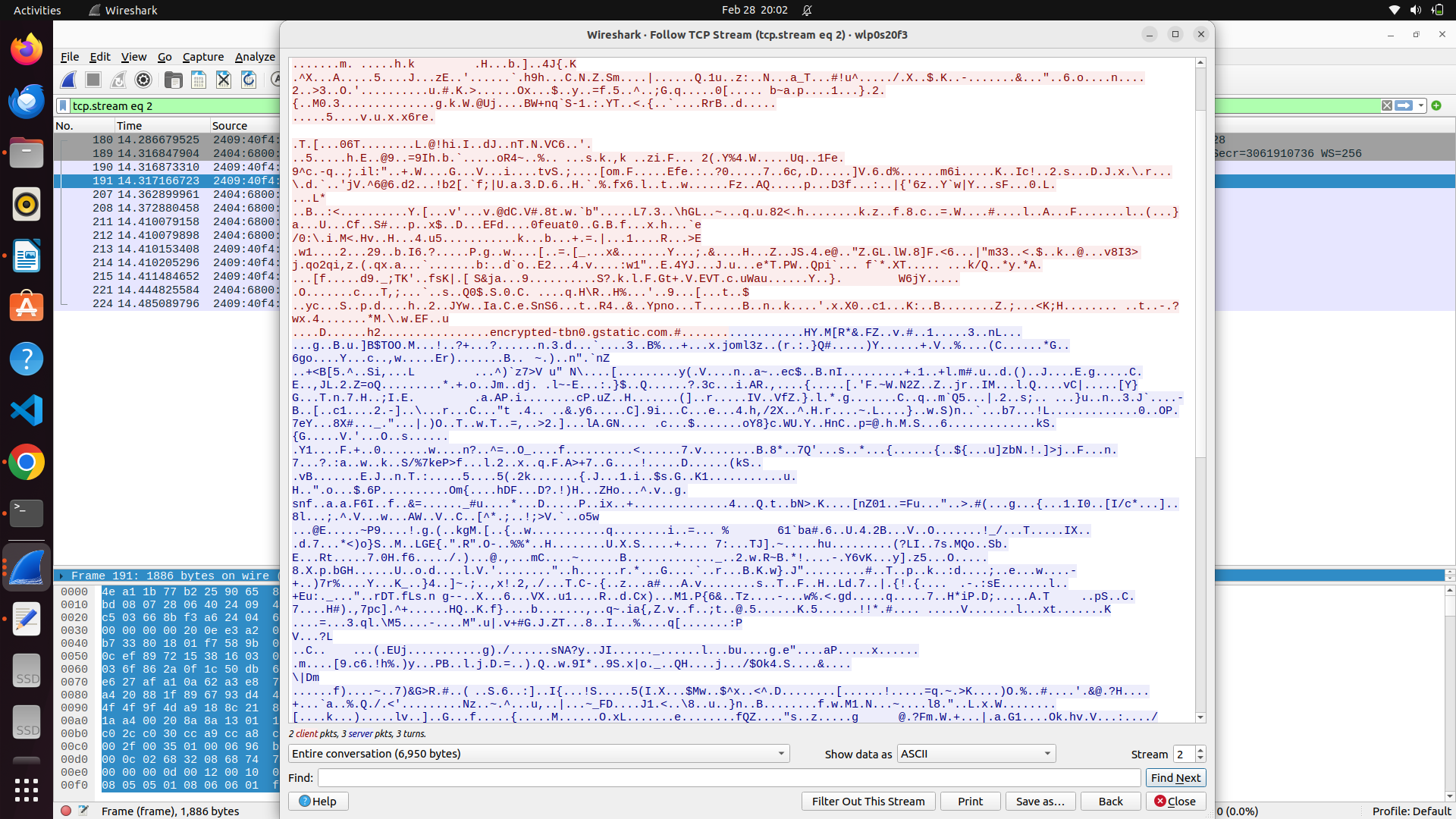
8. Wireshark packet capture can be stored as pcap or pcapng files that can be opened in most of the packet sniffing tools or softwares like tcpdump etc.



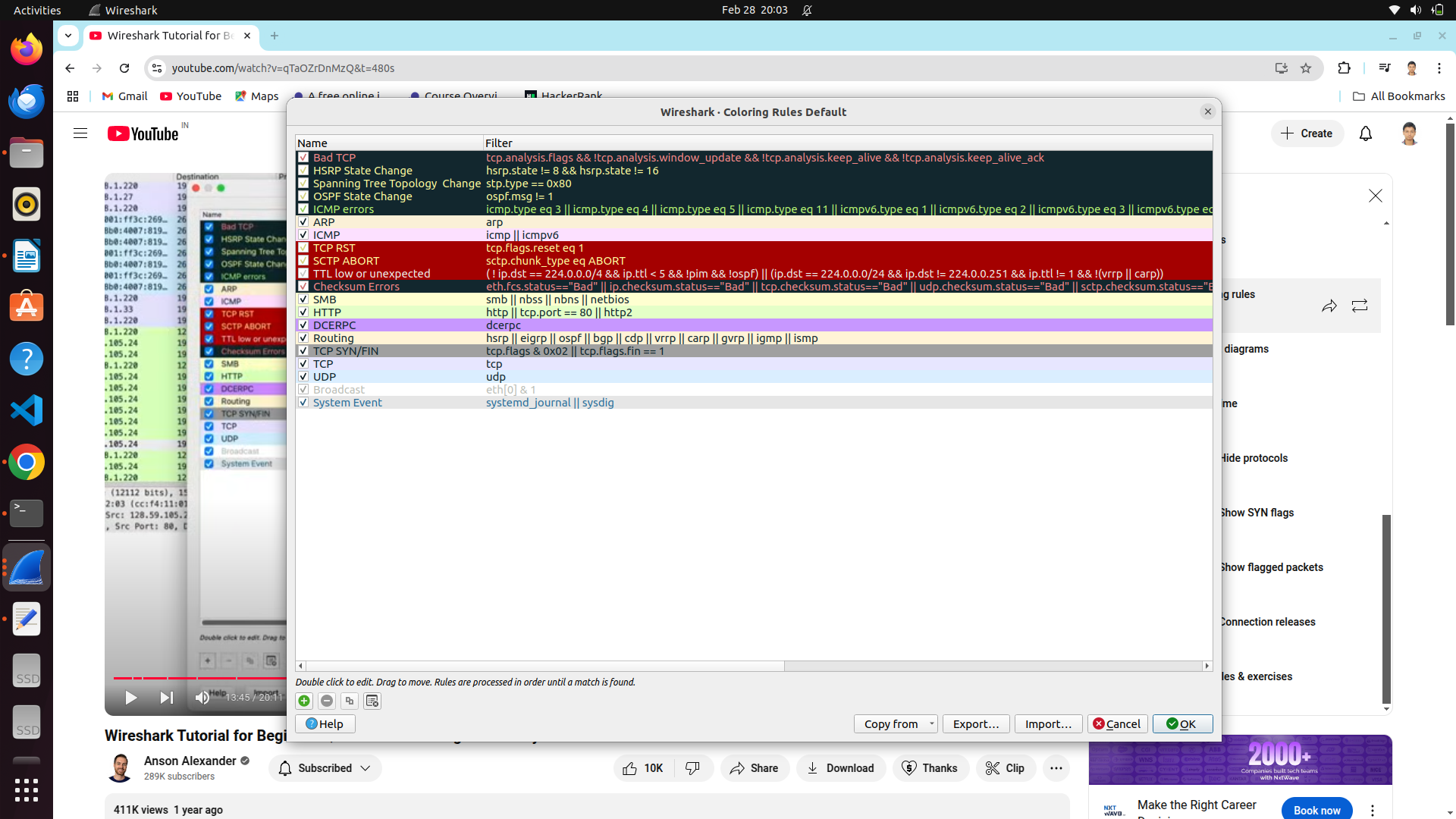
9. Here, a sample captured file is opened in wireshark itself and as like live captures, filters and other statistics can be applied as shown:



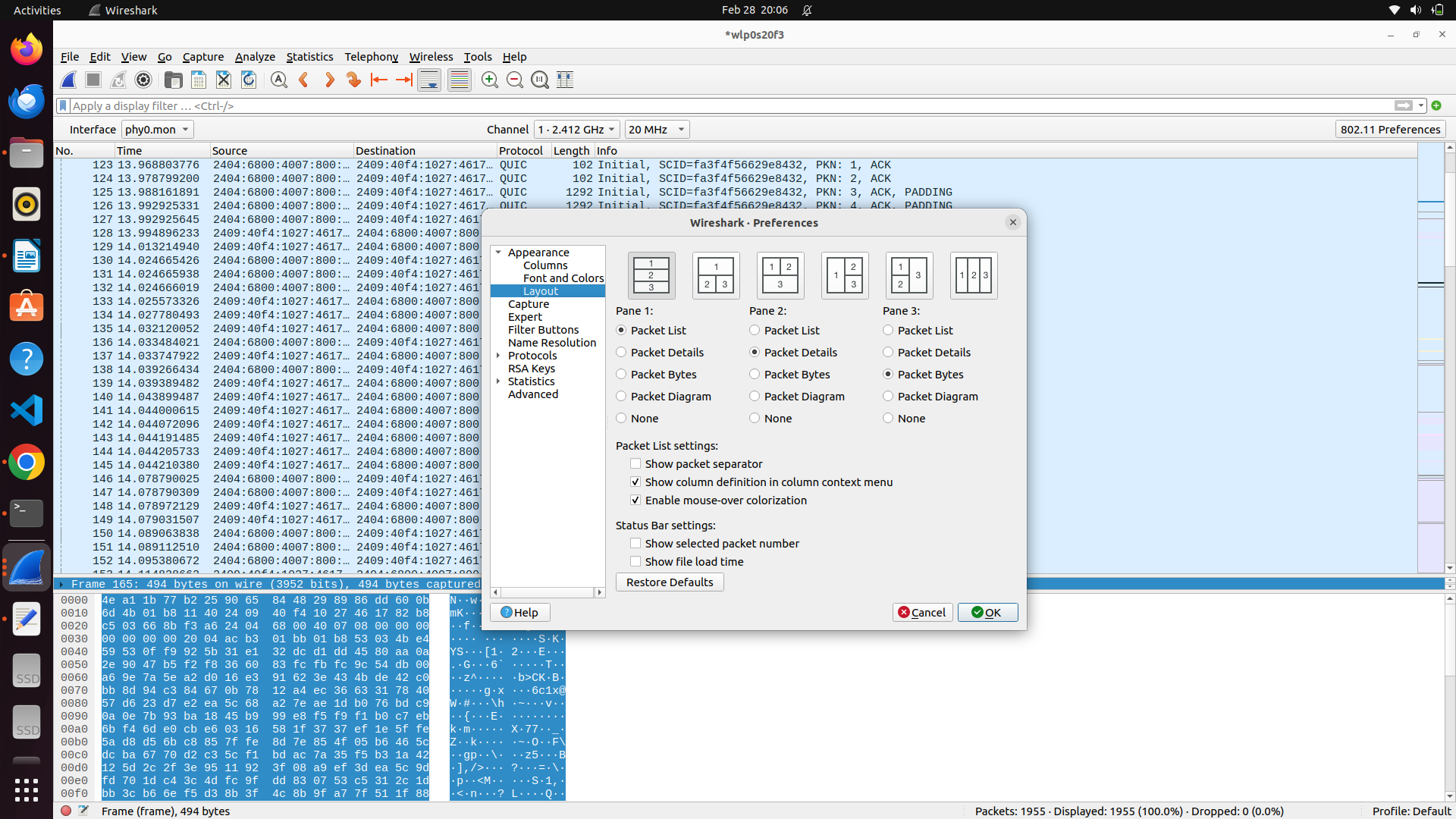
10. Here, demonstration of following the tcp stream conversation is shown: (since https packet is followed, all payload will be encrypted below)



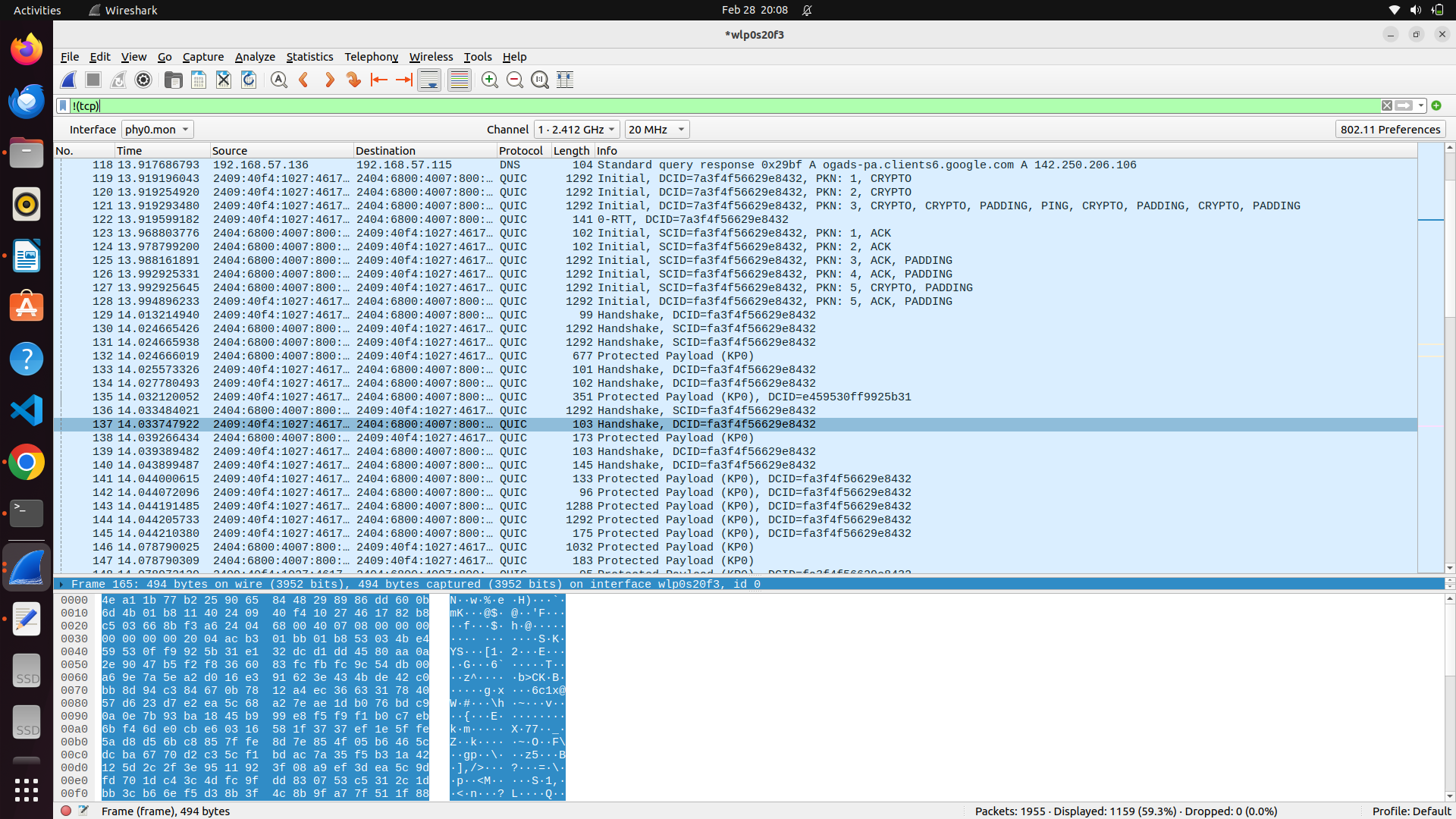
11. Wireshark follows its own colouring rule in showing packets like application data, bad request packets, conventional packets like handshakes, protocol related packets etc will be differentiated in terms of its colours and the details of colour differentiation and custom choices of colours for any event can be chosen as follows (under preferences option):



12. Layout of the packet capture window (by default, table showing the details of each captured packet followed by the protocol wise details and followed by payload display). The order can be changed and new options can be included along with existing packet related information and so on as shown (under layout option in preferences):



13. Filters can be applied in terms of negation such as neglecting TCP, UDP, packets with particular IP , particular port(s) etc as shown :



CONCLUSION :

Thus , Wireshark software is explored by capturing from intended network interface , applying different filters , using statistics option , understanding colouring rules , layouts , conversation filters , storing and retrieving packet captures.