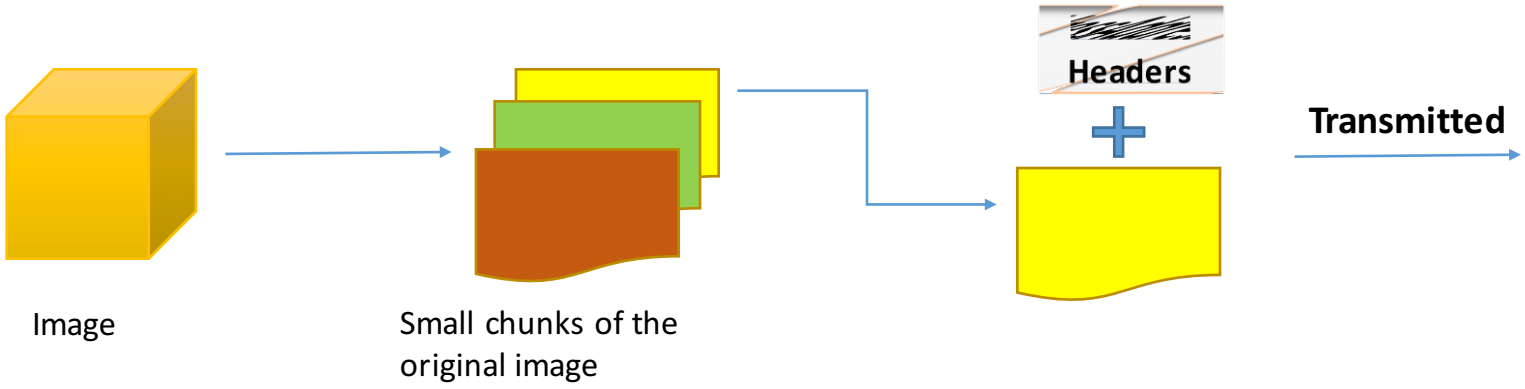
Stream of packets:

- There is a maximum size limit for the packet to be transmitted over the network.

- For Ethernet (the most common network technology), it is 1500 bytes.
  - 1460 Bytes of data payload + 20 Bytes of TCP header + 20 Bytes of IP header.

- A TCP packet can take only 1460 Bytes of data as a payload over Ethernet network. Therefore, the communication typically requires exchange of multiple packets between the source and the destination

- The payload to be transmitted is broken into smaller pieces to keep the packet size within limits. For example, to send a picture of 4 MB i.e. 4096 bytes, the picture will be segmented into smaller pieces and it will take more than one packet to send the picture.
- For an investigator it is important to capture multiple packets in order to make complete sense of the content being sent or received over the network.



Packet Capturing Tools:

Wireshark: *www.wireshark.org*

- The information being sent or transmitted over the network could be captured by the tools called packet sniffing or capturing tools.
- One of the most popular packet capturing tools is **Wireshark**. It can capture packets that are sent or received by the device.
- It can also analyse the packets captured by any other tool.

NetworkMiner http://www.netresec.com/?page=NetworkMiner

- Network Forensic Analysis Tool for Windows
- Can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc.

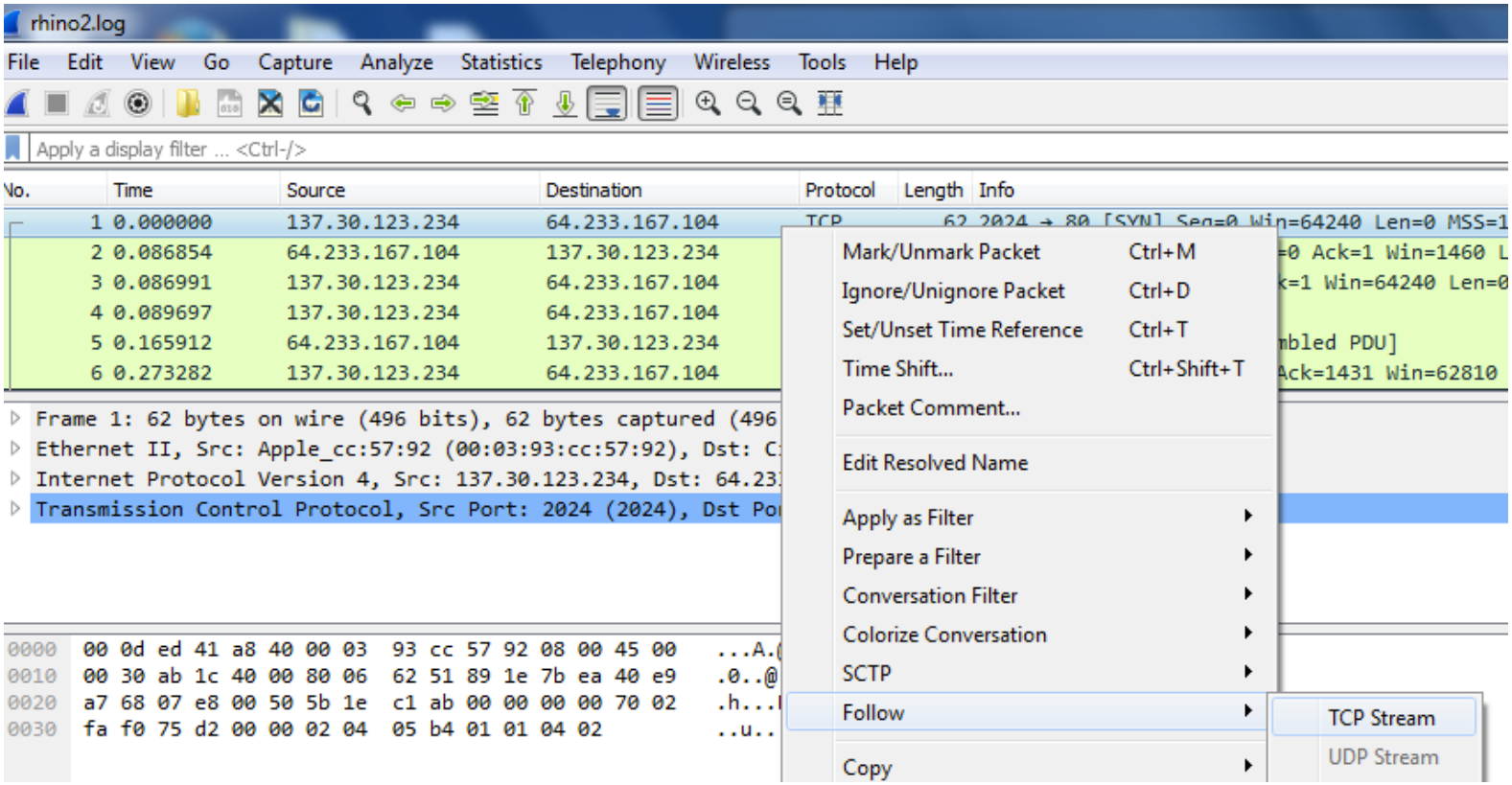
Wireshark Features:

- Devices may run multiple network dependent applications or services simultaneously. Therefore, A large number of packets are captured in a few seconds, which makes filtering very important for the investigator.

- Wireshark Display Filters show the packets of interest and hide all other packets for convenience.

- Wireshark lets you reassemble the data exchanged during a specific communication.
- One of the easiest way is to select the packet of interest, right click and select follow > TCP Stream.
    - This option will extract information and reassemble the data from selected stream.

TCP Stream


rhino2.log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 137.30.123.234 64.233.167.104
2 0.086854 64.233.167.104 137.30.123.234
3 0.086991 137.30.123.234 64.233.167.104
4 0.089697 137.30.123.234 64.233.167.104
5 0.165912 64.233.167.104 137.30.123.234
6 0.273282 137.30.123.234 64.233.167.104
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496
Ethernet II, Src: Apple_cc:57:92 (00:03:93:cc:57:92), Dst: C
Internet Protocol Version 4, Src: 137.30.123.234, Dst: 64.23
Transmission Control Protocol, Src Port: 2024 (2024), Dst Po
0000 00 0d ed 41 a8 40 00 03 93 cc 57 92 08 00 45 00
0010 00 30 ab 1c 40 00 80 06 62 51 89 1e 7b ea 40 e9
0020 a7 68 07 e8 00 50 5b 1e c1 ab 00 00 00 00 70 02
0030 fa f0 75 d2 00 00 02 04 05 b4 01 01 04 02
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
TCP Stream
UDP Stream

Exporting HTTP Objects