William Fu

Tisha Brown

4/24/18

WireShark Lab 5

(I couldn’t get my wireshark to run for some reason, so I used the trace for download using the link you gave in the question packet)

1. IP of trace: 192.168.1.102
2. Identifier BE of trace: 768 (0x0300)
3. Size of IP header: 20 bytes in IP header. 36 bytes in payload cause the total is 56. 56-20= 36.
4. Fragmented? No, fragment offset = 0
5. Fields that change in the IP datagram: Frame, Identification, and Time to live
6. Fields that stay constant/must stay constant across IP datagrams: version, header length, source + destination, protocol.

* Source and destination are always the same since we are sending back and forth from the same locations.
* Protocols and header length are the ICMP packets.
* Version is the same as all are using IPv4

Fields that must change: identification, time to live, header checksum

* IP packets must have diff ids
* Time to live traceroute increments each subsequent
* Header changes so much checksum

1. Describe pattern in values of Identification field: pattern is IP header id fields go up by 1 with each ICMP echo request
2. Identification field: 0x9d7c (40316) TTL: 64
3. Identification field changes for all ICMP TTL replies bc ID field is a unique value. If two or more IP datagrams have the same id value then it means that these IP datagrams are fragments of a larger one
4. Yes, it is across more than 1 ip datagram