

17. 9. 25 5. capturing and analysing packets with wireshark

Aim to perform experiments on packet capture tool wireshark.

Packet sniffing

* Sniffing messages being sent/received from network card of computer from different programs.

* possible programs → never sends packet, it's to packets

Tool

wireShark.

Description

Tool wireShark or network analysis tool formerly known as Ethereal, captures packets in real time.

uses

- * Network administration
- * Network Security Engineers
- * Developers debug protocols
- * People learn network protocols / internals

Packet list pane

packet list pane displays all packets in current capture file, comes down to one packet in capture file.

Packet details pane

packet detail pane shows current packet frame pane shows protocol fields and protocol of packet selected in packet list pane.

Packet By its port

Packet by its port shows data of the current packet selected in the packet list now in a hexdump style.

Color coding

You could see probably highlighted packets in a variety of different colors. Wireshark uses colors help you identify the types of traffic at glance. By default, light purple is TCP traffic, light blue is UDP traffic filtering packets

If you're trying to inspect something specific, such as traffic a program sends over phone or some. Still you will likely a large amount of packets to sift through.

Capturing and analysing packets

Procedure

1) Select local area connection in wireshark

2) Go to capture → options

3) Select stop capture after 10 packets

4) Then click Start capture

5) Save packets.

I create filter to display by TCP/VDP packets, unspec packets.

- Select LAN in wireShark
- Go to capture → option
- Select Stop capture
- Search Tap packets in search bar
- To see flow graph.

Check statistics → flow graph.

→ Save packets.

Procedure

- Select LAN in wireShark
- Go to capture → option
- Select Tap packets in search bar
- To see flow graph.
- Save packets.

2) Create a filter to display only ARP packets

Procedure

- Go to capture → option
- Selected Stop capture Auto for 100 packet

Then stop capture and search and save.

After saving file do right click and select image as always.

Output

of file 000.garp2

Time	173.478 - 75.233 sec	Host	localhost
Source	8d0fa7188.10.1.101:5001	Dest	dns.9009.10.1.101:53
54936	134936 http/room/6222/3028	Command	
54936	1400400m(5222)	5028	7070:54936 ->
55141	< Application Data		http/room(5222)
55141	< Application Data		stop/room(5222)
55141	< Application Data		-> 56036 Pack
55141	< Application Data		HTTP/2 Application
55141	< Application Data		Pattern
55141	< Application Data		Pattern
55141	< Application Data		Pattern
55141	< Application Data		Pattern

o and port 5001 is opened

now blocks mapping Algo is run go back

it go forward a block changed state to

blocked blocks like bad block reward

and blocks left in it Aug-19 can see 2

(Pending nodes) expected

blocks blocks mapping which

These created 6001 is used to handle
and inspect packets

blocks bad blocks in which
left untagged no correct file

2492 blocks or all gone or 6013 of

6000 of this good all known for
blocks at regular basis

so we can see that the blocks are