Buctical-5

on 'packet capture tool: wireshork. Experiments

atis was wineshork's fitters cov

1) Promissions mode - It is a

our hade we down w

wineshark:

wireshork, a metwork analysis tool formely known as etherocal, captures packed in ord time and display them in human readable formert. wireshork includes filters, colour coding and other features that let you dig deep into methorik traffic and inspect observations: individual packets.

capturing packets: It shows to be not to be no

After downloading and installing evireshark but it and double click the name of a network interface.

colour coding:

wireshark uses tolows to help you identify the type of traffic at a glance - By default, light pumple is Ter truffic, light blue is wap truffic and black identifies packets with errors.

Filtering packets: something specific such as the toughic a progress when phoning home. It helps to close down out other applications using the network . so you are a starge will likely have a large will dikely have a large amount of packets to shift through. That's where wireshark's filters come in.

Inspecting Packets:

click a packet to select it and
you san dig down to view its

details.

observations:

- i) Poromiscuous mode It is a configuration of a network interface card where we is set to pass all braffic it vicaives to CPU vicition then just the packets additioned to it.
- 2) ARP Rackets do not have ver stransport layer header. It operates at desta link layer of os; model and its purpose is to may an 1P raddress. By a MAC raddress.
- 3) Dus uses both 1cp and use usp transport layer protocols
- 4) HTTP uses part humber 80.

1P address is an address bransmission of data to all 5) A broadcast that allows has to on a network. and coorection using HAMMERNER code conept. moste a test own , to input data astron and voiding error correction feedure. o Imput 6 sender fire whould be a test of ony length. persogram should convert the tweet to binary. · Apply harming reads concept on the binary dedet and add redundent blo 6 it. balles this giple in a file called rehannel. Being program: Januaria mary Lugar brown channel apply hamming code on the binary date. Result: Thus experiment on packet explore 6001. wrieshark is performed and observations are noted de balance set success sets. Our 121. Alesto general de troums.