

Tool Exploration –Wireshark

- EXP - 17 -

- Wireshark -

key features

1. packet capture : captures live network traffic from various interfaces
2. protocol analysis : supports hundreds of protocols
3. filtering : offers powerful filters to isolate specific packets or traffic types
4. visualization : displays packets details with their actual layers.

Use cases :

1. network troubleshooting :
 - diagnosing slow network speeds
 - identifying bottlenecks
2. security analysis :
 - detecting malicious traffic
3. protocol study :
 - understanding packet structures, communication flows