Task 5: Capture and Analyze Network Traffic Using Wireshark.

Objective: Capture live network packets and identify basic protocols and traffic types.

Tools Used: Wireshark (packet analyzer)

Protocol	Purpose
dns	Resolving website domains
ICMP	Network diagnostics (ping)
tls	used in HTTPS encryption

Filters Used

icmp
dns
icmpv6
igmp
Arp

Observations

DNS traffic shows a domain lookup for hackthebox.
ICMP and ICMPv6 indicate active ping operations.
TCP is common for most traffic

Learnings

Gained hands-on experience with network protocols.
Learned how to use filters to isolate packet types.
Observed both IPv4 and IPv6 traffic in a real environment.