# Kerberos Traffic Analysis

Reference: <https://www.golinuxcloud.com/kerberos-auth-packet-analysis-wireshark/>

* Activate this under Edit – Preference (in Wireshark)

A screenshot of a computer

Description automatically generated

* Find the AS-REQ request



* Type AS-REP request:

A screenshot of a computer

Description automatically generated

* Hash and type of hash(18 is the ASREP type):



* And lastly the REALM and USERNAME:

A screenshot of a computer

Description automatically generated

* Knowing this you should be able to find the hashtype in hashcat:



* And componing the hash like

$krb5pa$18$username$realm$cipher