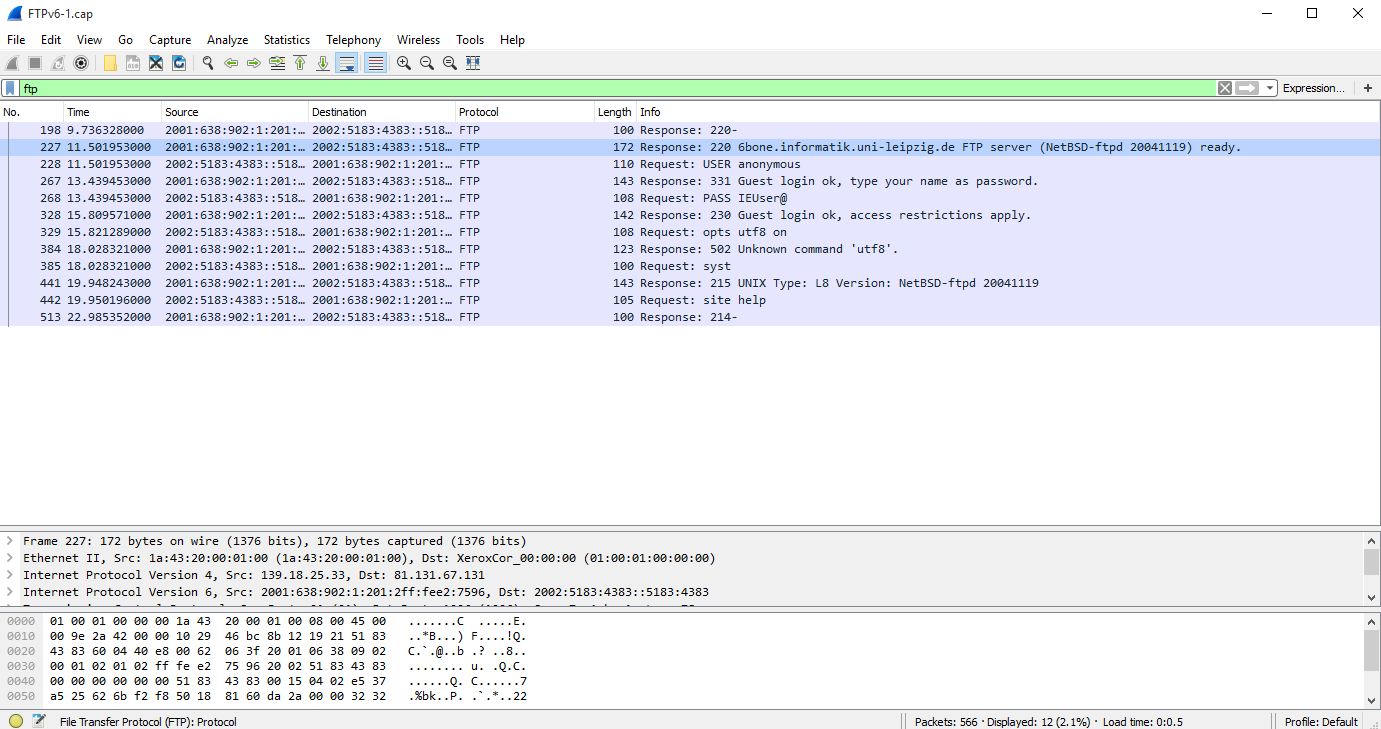
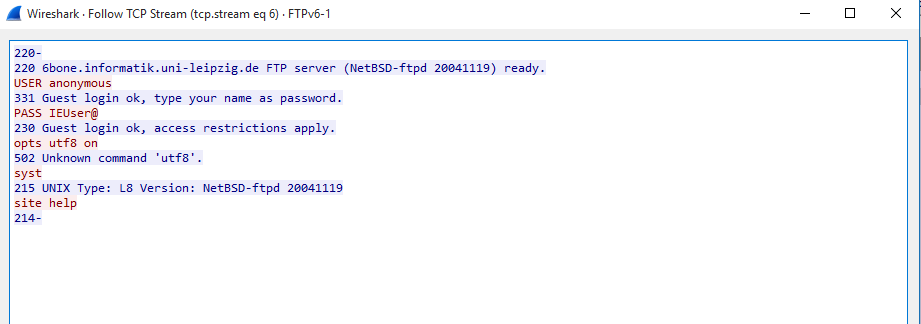
Captures

FTP

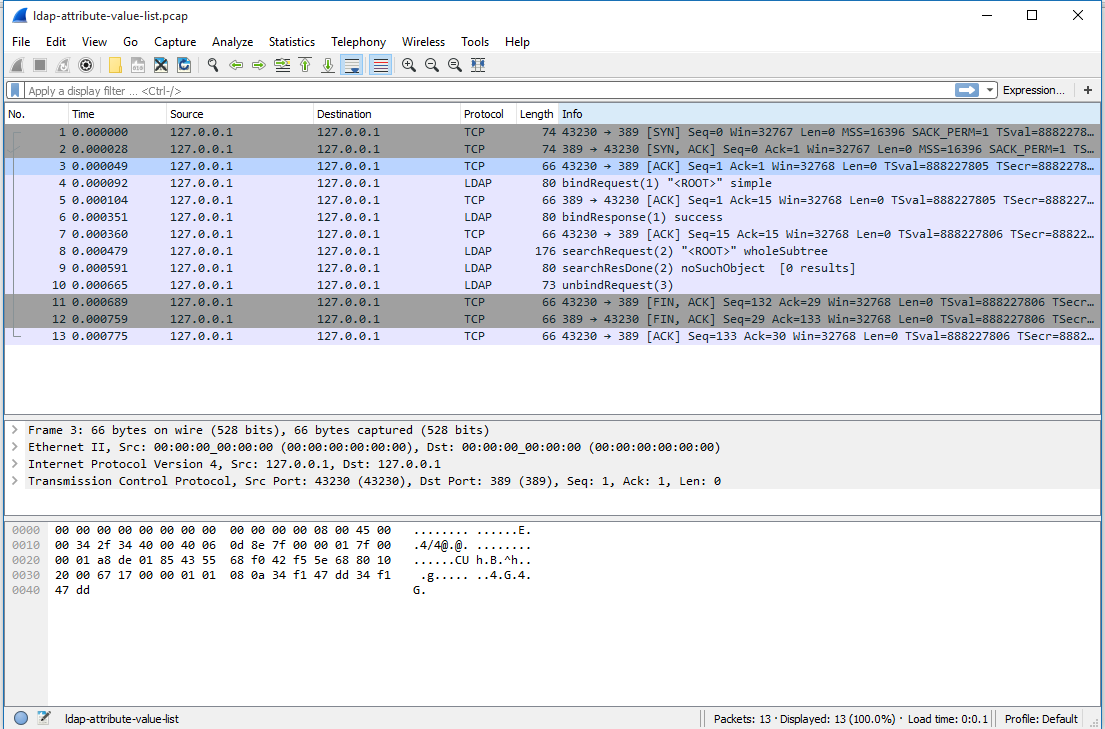


This is a filtered conversation of packets using the FTP protocol. It is also good to note that this communication is using IPv6, however you can see that these machines use the Ipv4/Ipv6 dual stack and that this information can be found looking at the frame.

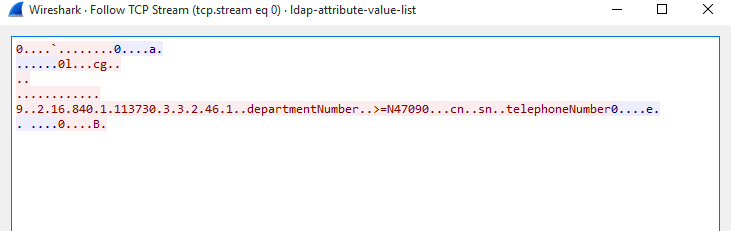


When we follow the packet stream, we can see that this FTP server has not used any security extensions, and that this information is in plaintext. This is not ideal as someone on the line, using a MiTM (man in the middle) attack could easily gain access to this FTP server.

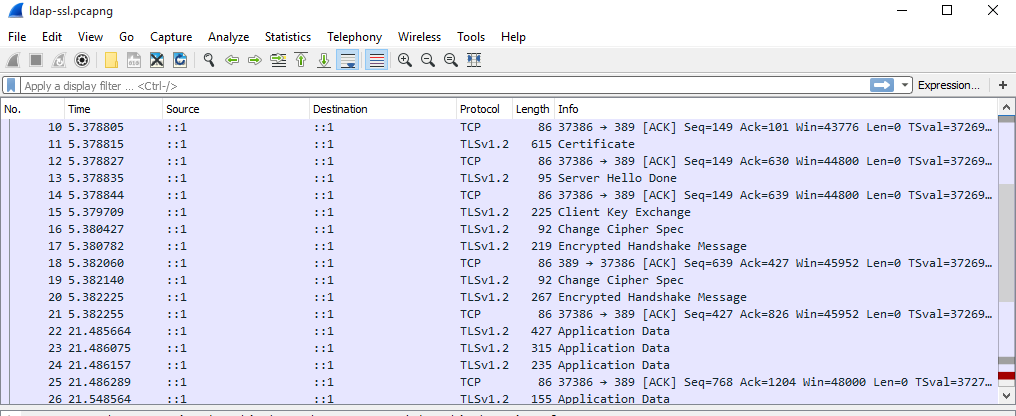
LDAP



Under the info tab we can see that this set of packets captures is performing an LDAP search command. And after we look at the TCP stream, we can find out that it is returning a list of attributes.

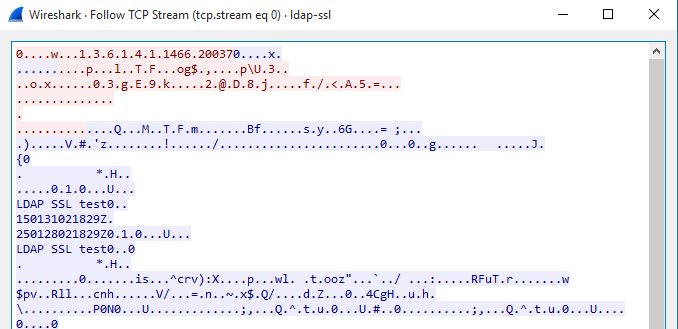


This is an example whereby this LDAP server has not implemented SSL, and results can be seen as plaintext. The example below will show what happens when SSL is implemented.

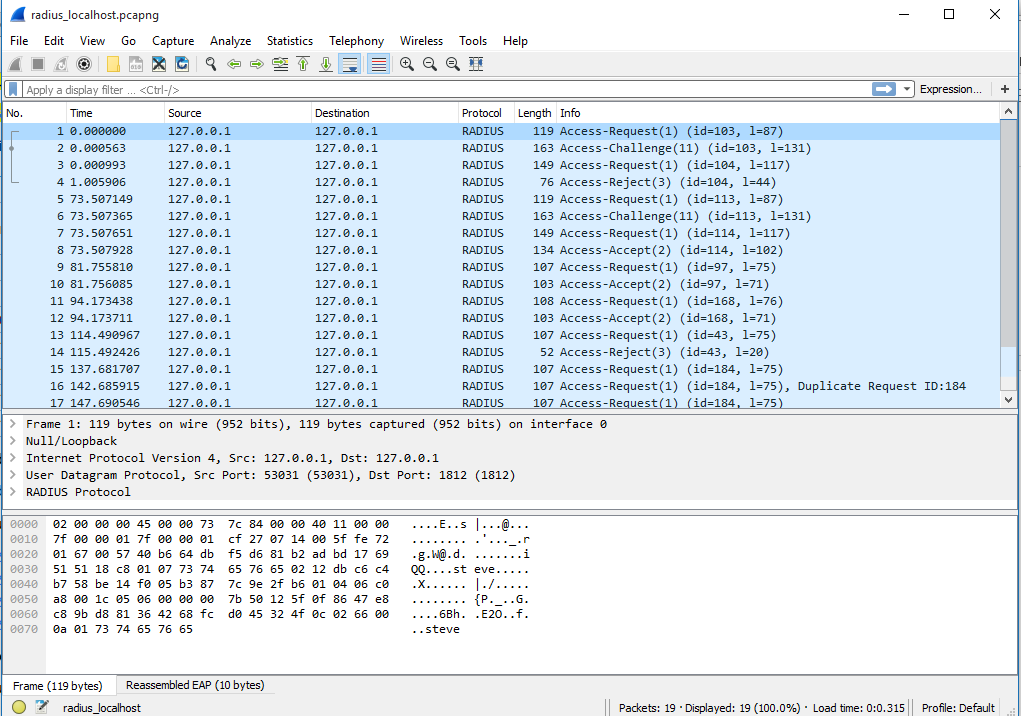


No longer is it possible to tell what type of command requests are being issued such as Bind, Search etc. These will all results in Application Data field in the info tab.

Following the TCP stream will lead nowhere now that the information is encrypted. Below is a small sample.



RADIUS



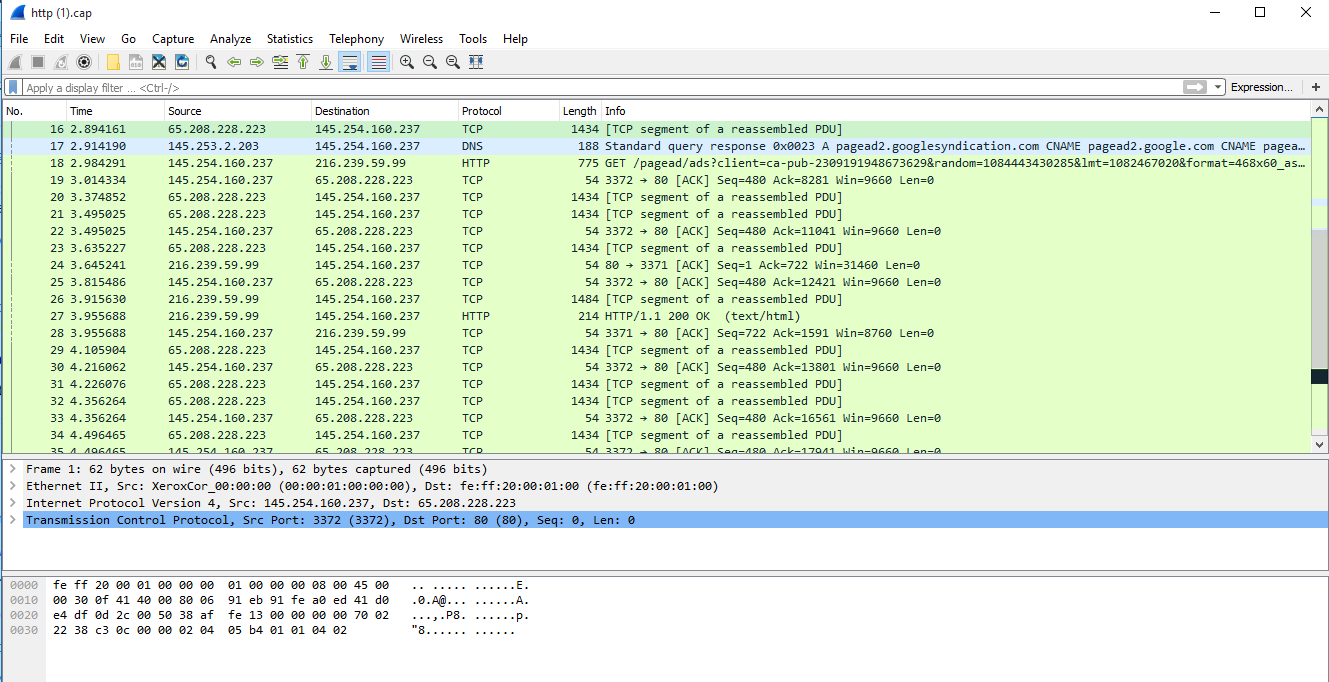
By looking at the capture we can tell what type of actions are. As mentioned in the vulnerabilities segment for RADIUS, an attacker can look a valid Access-Accept and try to break it offline. Or try to do a replay attack by using the same segment.



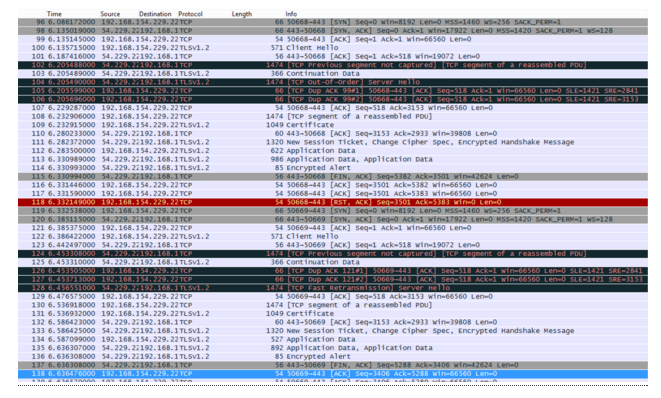
The above is a result of following the stream for an Access-Accept. Most of the information is hidden away from plain sight.

SVN

Since Subversion is an Apache service, we can usually find it running alongside an HTTP service.To filter out for the ra\_svn protocol in Wireshark, we must use a tcp port filter on port 3690.



The info tab should pull up information regarding requests from clients as well as. Below is an example of implementing SSL with SVN, and capturing the conversation of a commit.



Due to a misconfiguration in the http.conf with no KeepAlive statement, even though it is the same IP making the commits, every 10kb of data has to redo the SSL handshake making it run very poorly.

http://serverfault.com/questions/728509/svn-over-ssl-many-reconnects-on-commit