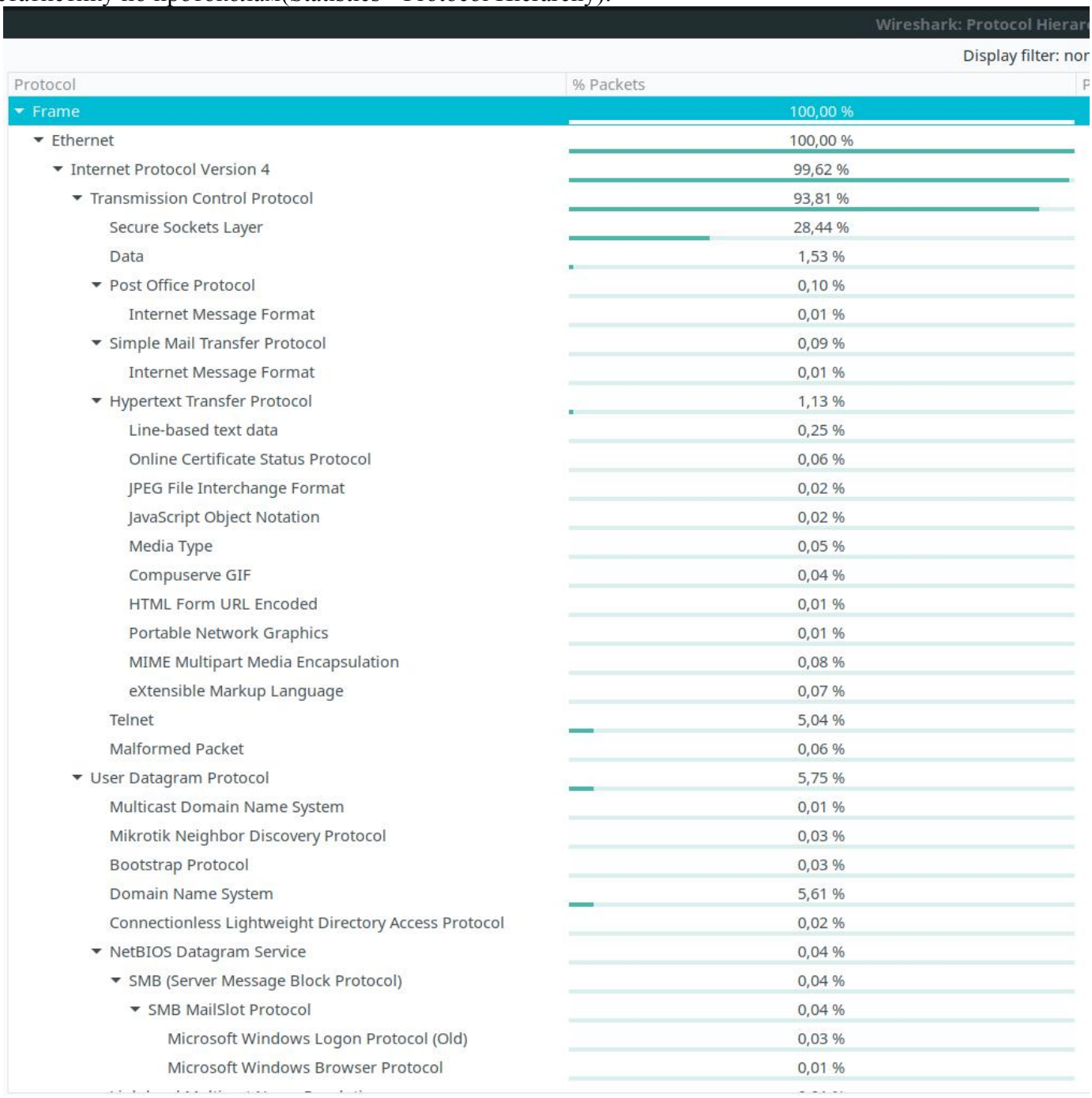
Задание является классическим с точки зрения сетевой форензики и исследования дампов трафика. В качестве подсказки будет название таска “ТЕЛСЕТ”. Первоначальной точкой для решения может являться:

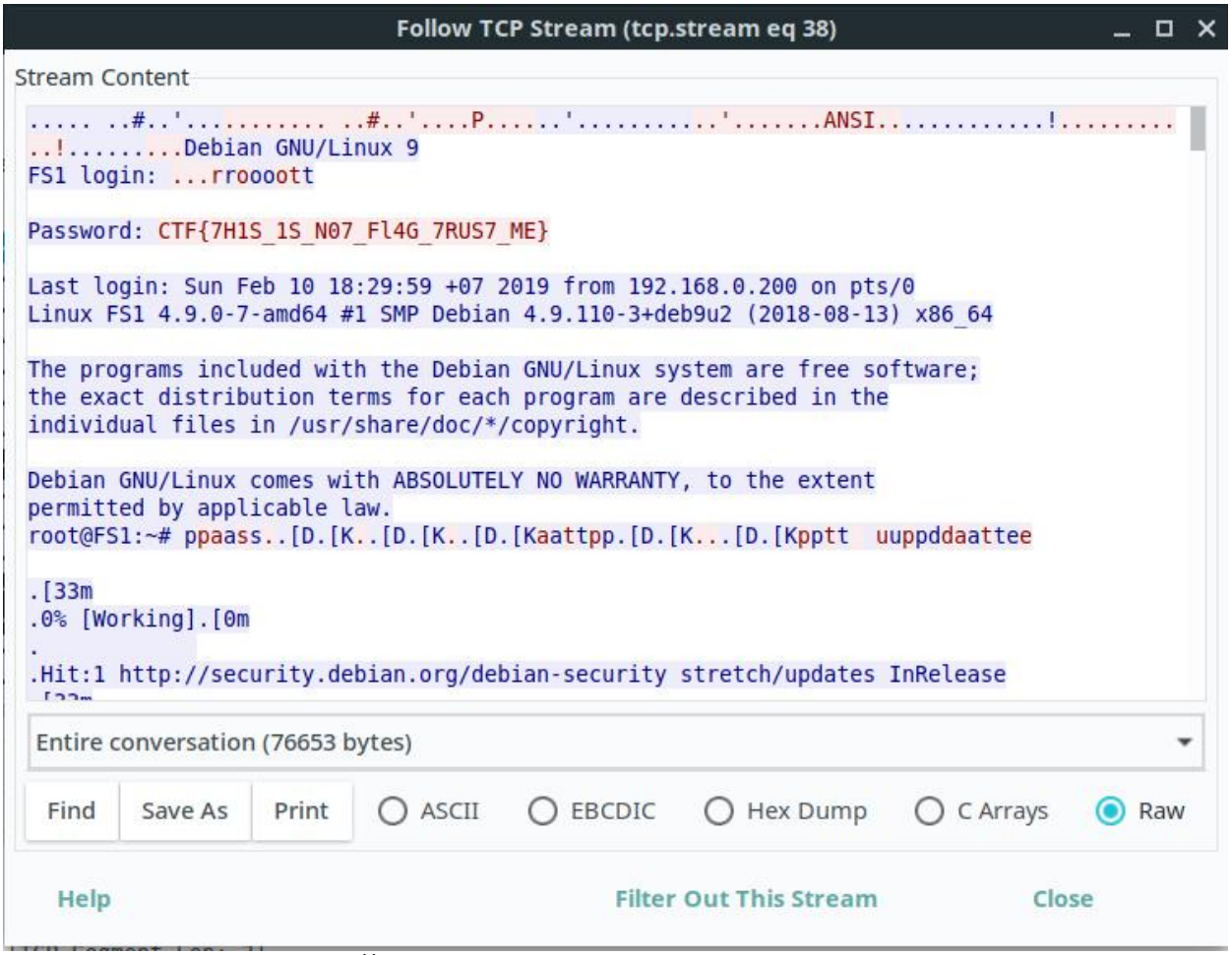
1. (Те, кто любят статистику и увидят что так можно и кто любит походить по меню) Взглянуть на статистику по протоколам(Statistics->Protocol Hierarchy):



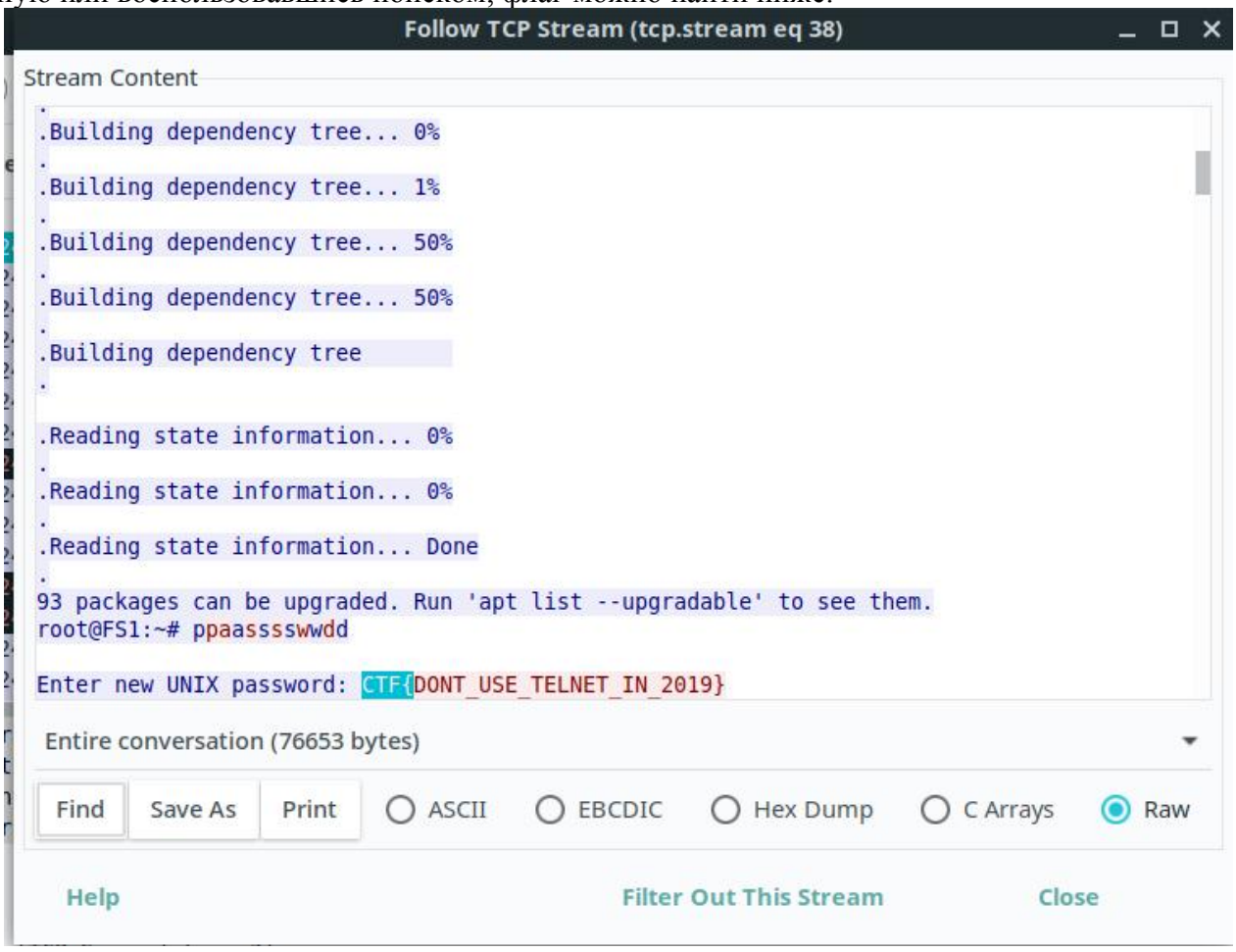
Protocol	% Packets
Frame	100,00 %
Ethernet	100,00 %
Internet Protocol Version 4	99,62 %
Transmission Control Protocol	93,81 %
Secure Sockets Layer	28,44 %
Data	1,53 %
Post Office Protocol	0,10 %
Internet Message Format	0,01 %
Simple Mail Transfer Protocol	0,09 %
Internet Message Format	0,01 %
Hypertext Transfer Protocol	1,13 %
Line-based text data	0,25 %
Online Certificate Status Protocol	0,06 %
JPEG File Interchange Format	0,02 %
JavaScript Object Notation	0,02 %
Media Type	0,05 %
Compuserve GIF	0,04 %
HTML Form URL Encoded	0,01 %
Portable Network Graphics	0,01 %
MIME Multipart Media Encapsulation	0,08 %
eXtensible Markup Language	0,07 %
Telnet	5,04 %
Malformed Packet	0,06 %
User Datagram Protocol	5,75 %
Multicast Domain Name System	0,01 %
Mikrotik Neighbor Discovery Protocol	0,03 %
Bootstrap Protocol	0,03 %
Domain Name System	5,61 %
Connectionless Lightweight Directory Access Protocol	0,02 %
NetBIOS Datagram Service	0,04 %
SMB (Server Message Block Protocol)	0,04 %
SMB MailSlot Protocol	0,04 %
Microsoft Windows Logon Protocol (Old)	0,03 %
Microsoft Windows Browser Protocol	0,01 %

2. Полистать трафик, увидеть Telnet
3. (для умных и кто любит походить по меню) Так как речь о пароле, поискать пакеты(Edit->Find Packet) по слову “Password”.
4. Догадаться, что речь о Telnet

Человеку, малознакомому с CTF и Wireshark, наверняка придется погуглить ключевые фразы. Было проверено несколько статей из выдачи “wireshark ctf” “wireshark site:habr.com”, описывающие базовые принципы и методы анализа трафика, а также различный функционал, например “Follow TCP Stream”:



По заданию надо найти НОВЫЙ пароль от сервера, таким образом это небольшая обманка. Пройдя вручную или воспользовавшись поиском, флаг можно найти ниже:



Флаг: **CTF{DONT_USE_TELNET_IN_2019}**