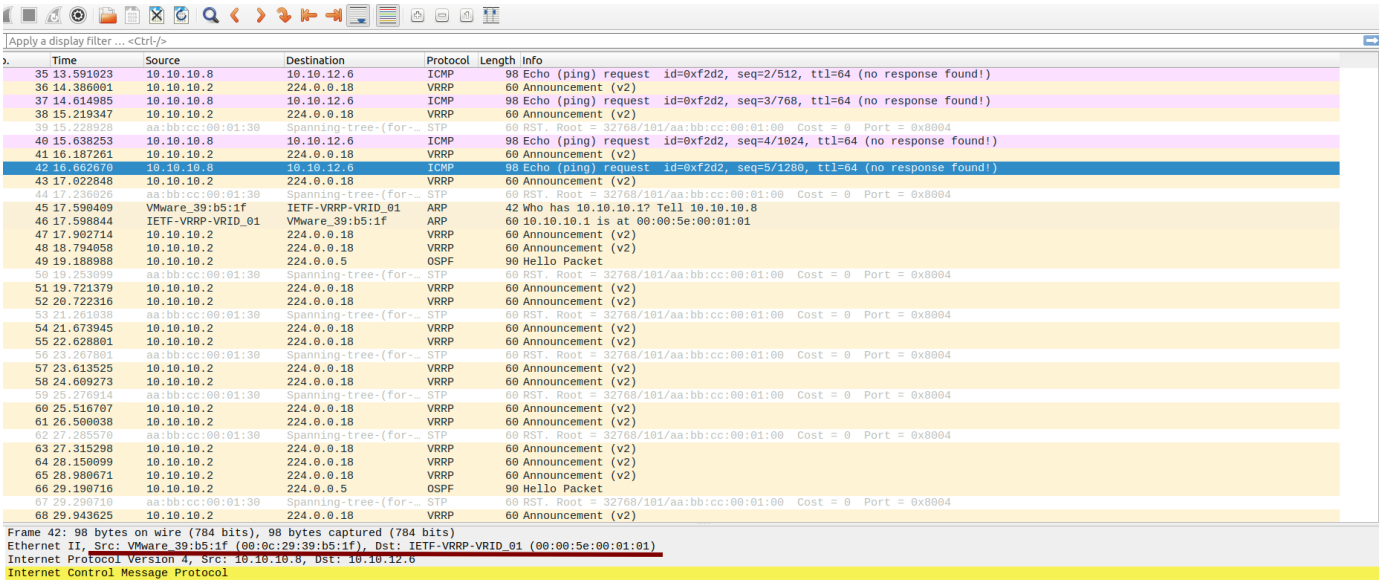
Анализ сетевых Дампов

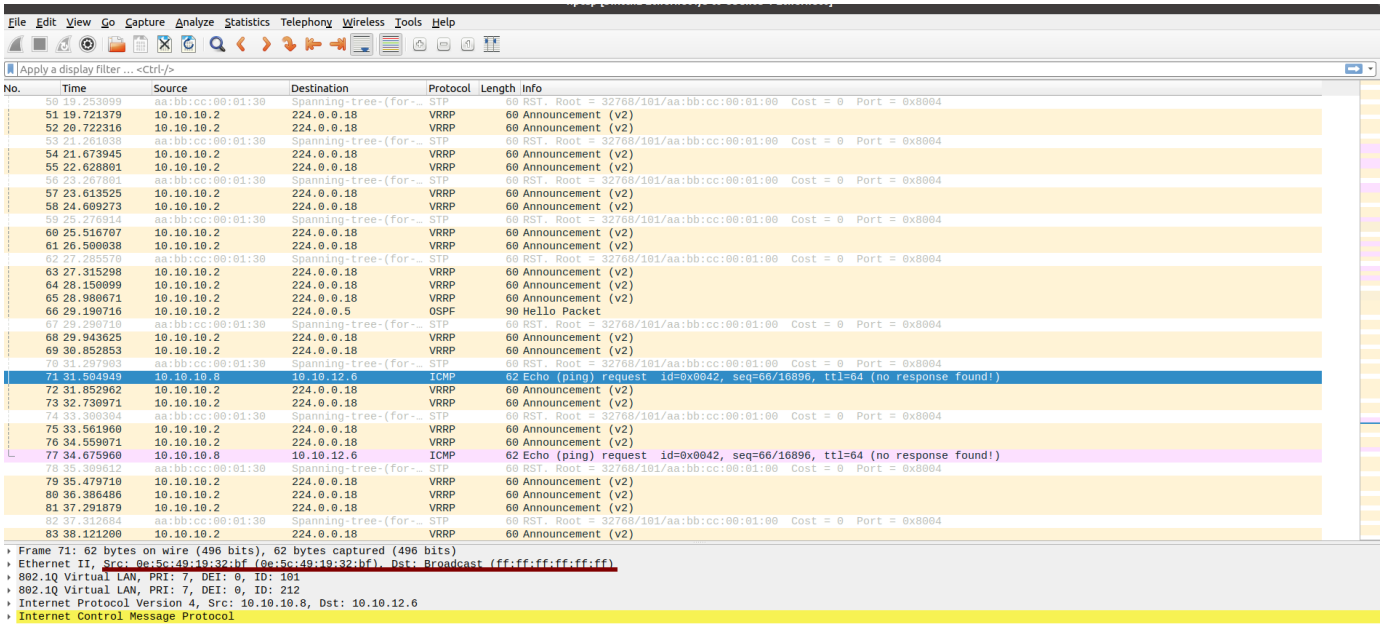
Dump №1

Извиняюсь что после делайна, в предыдущем не успел вообще ничего проанализировать. Вот сел в выходные, и решил скинуть. Может зачтется за исключение штрафных баллов.

На первом дампе можно увидеть протокол VRRP. VRRP (Virtual Router Redundancy Protocol) — сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию. Фактически, если один маршрутизатор(мастер) выйдет из строя, подключится запасной. Два физических маршрутизатора объединяются и создают виртуальный маршрутизатор, ip которого проставляется у хостов как Шлюз по-умолчанию.
P.S. Думал какая то атака на этот протокол, но в первом дампе меня лишь смущает одинаковые MAC адреса ip 10.10.10.2 и 10.10.12.6.
10.10.10.2 по идее мастер роутер, которые отправляет VRRP сообщения остальным о своем состоянии. Ему назначается вируатльный MAC адрес с началом 00:00:5E:00:01:{VRID(01)}.
Так вот, на пинге от 10.10.10.8 до 10.10.12.6 мы видим одни Мак Адреса на запросе 43.



А на следующем пинге на запросе 71 у src другой mac адрес, а dst - широковещательный.



То есть пинги летят всем устройствам в сети. А получателем станет MAC адрес, который появился в src - 0e:5c:49:19:32:bf
Выглядит как ICMP flood атака.

Dump №2

На втором дампе видно, что происходит DDoS SYN сообщениями по протоколу TCP. Жертва должна отвечать пакетами SYN/ACK. Атака называется SYN-FLOOD.