

заходим на сайт <http://nowa.cc>, с него авторизация уходит методом “Post”

в программе “Wireshark” также можно найти отправку пароля на сайт, если ввести в строке поиска : http.request.method==POST

IP address сайта : 77.120.105.164 –> ip.addr == 77.120.105.164 – вводим в строку для поиска запросов на сайт

находим запрос: 2618 134.884261 192.168.101.182 77.120.105.164 HTTP 1410 POST /login.php?do=login HTTP/1.1 (application/x-www-form-urlencoded)

открываем список и видим

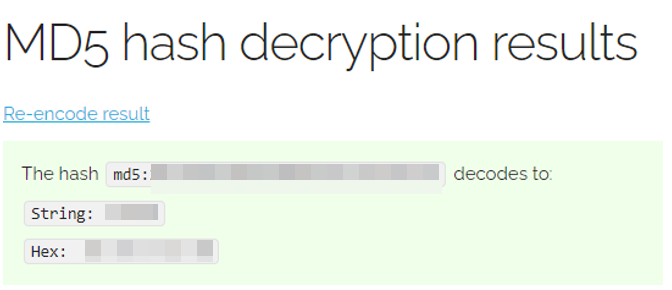
Form item: "vb\_login\_username" = "\*\*\*\*\*\*\*\*"

и ниже зашифрованный пароль методом “md5”

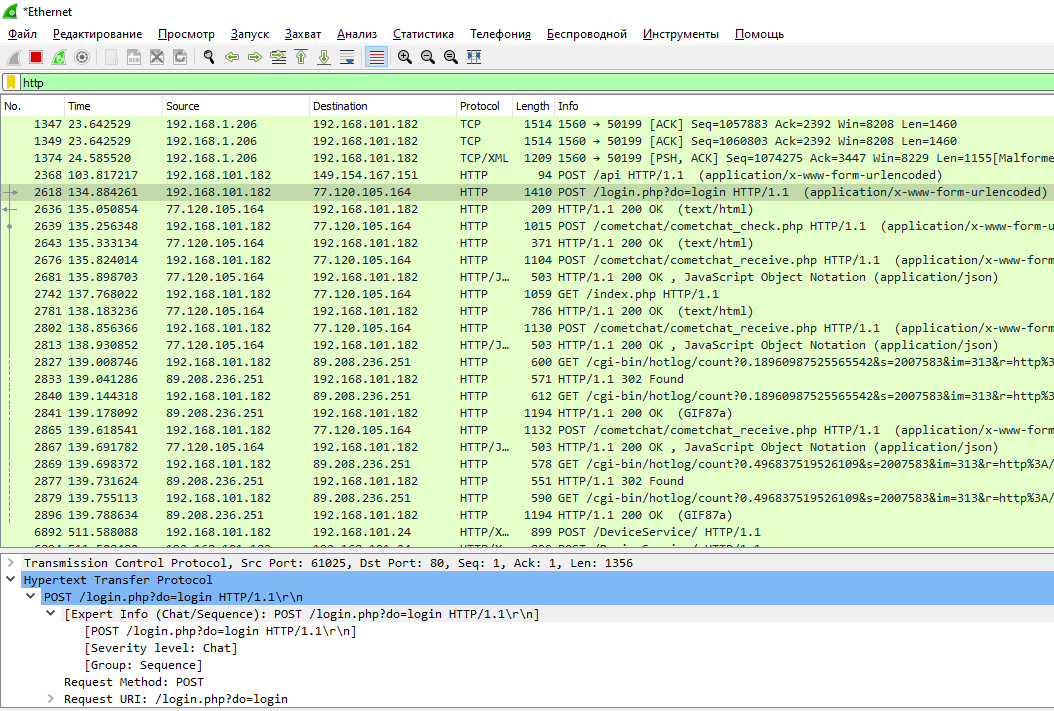
Form item: "vb\_login\_md5password" = "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

с помощью сервиса: <https://md5.web-max.ca/>

легко его раскодируем☺



можно группировать запросы по HTTP:



можно также пофильтровать другие протоколы, например icmp ssh ospf в приложенном pcap файле 