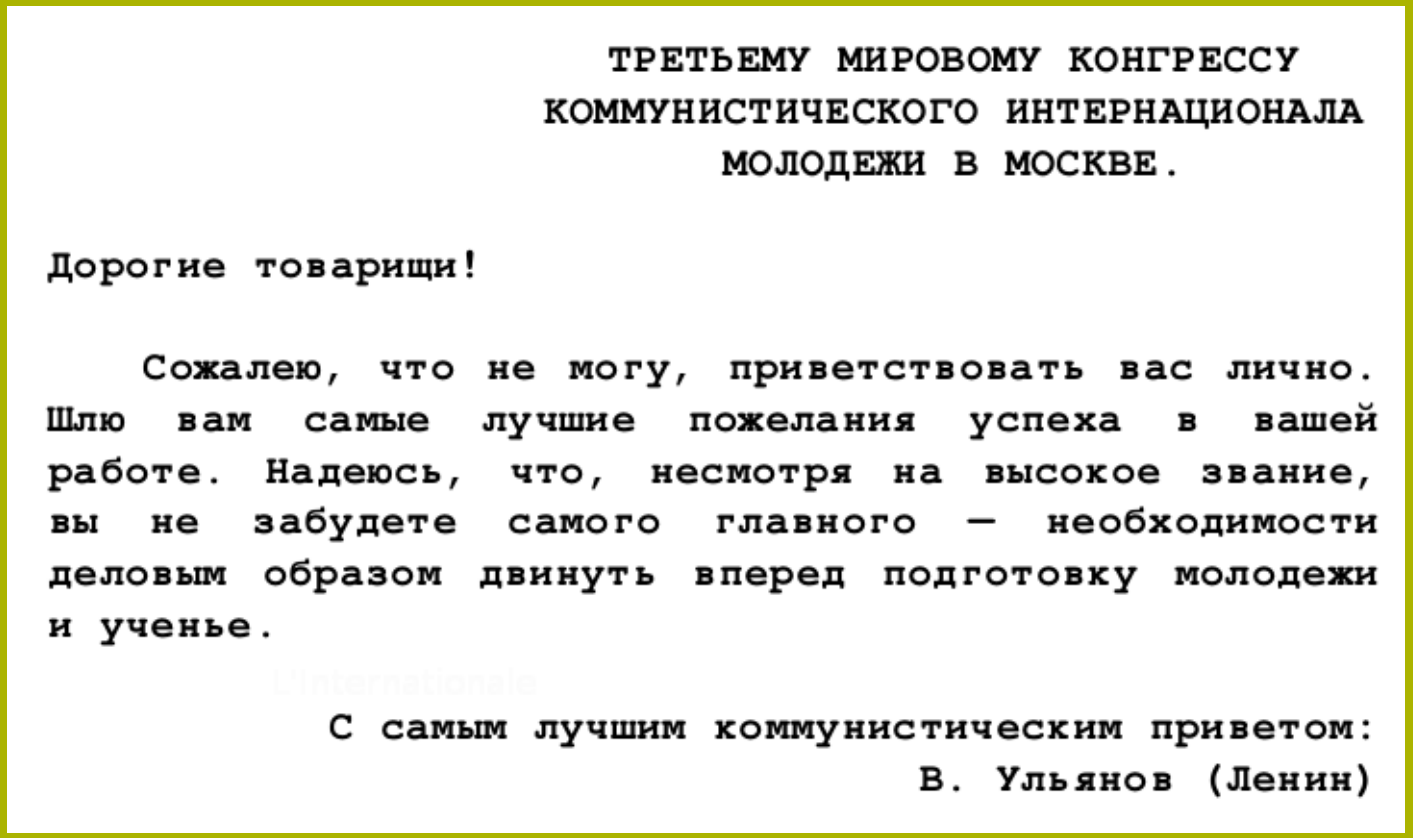
Stegano 400

CTC

Covert timing channel

Участники получают файл LeninLetter.png, который являет собой письмо В. И. Ленина к молодежи.



ТРЕТЬЕМУ МИРОВОМУ КОНГРЕССУ
КОММУНИСТИЧЕСКОГО ИНТЕРНАЦИОНАЛА
МОЛОДЕЖИ В МОСКВЕ.

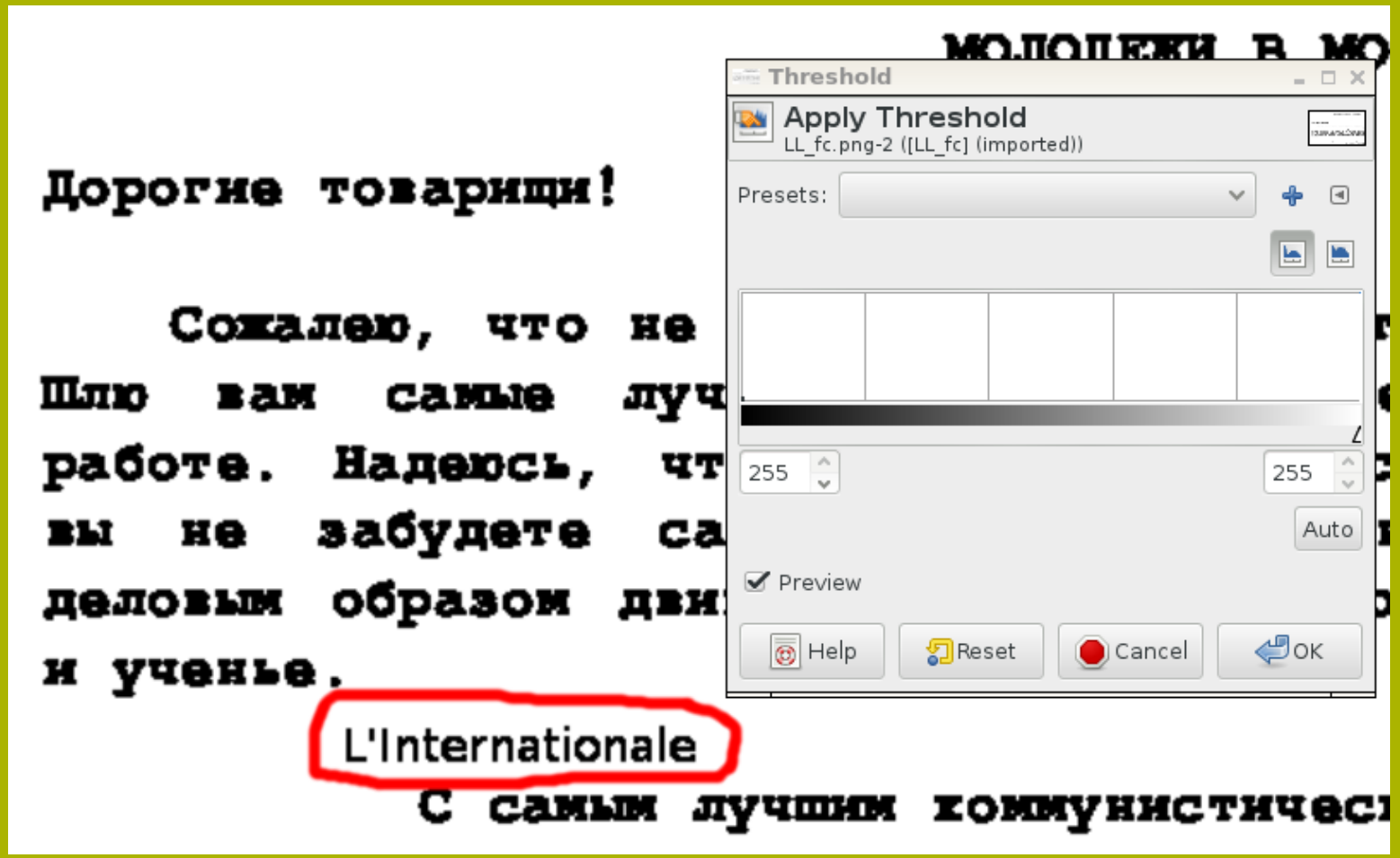
Дорогие товарищи!

Сожалею, что не могу, приветствовать вас лично. Шлю вам самые лучшие пожелания успеха в вашей работе. Надеюсь, что, несмотря на высокое звание, вы не забудете самого главного — необходимости деловым образом двинуть вперед подготовку молодежи и ученье.

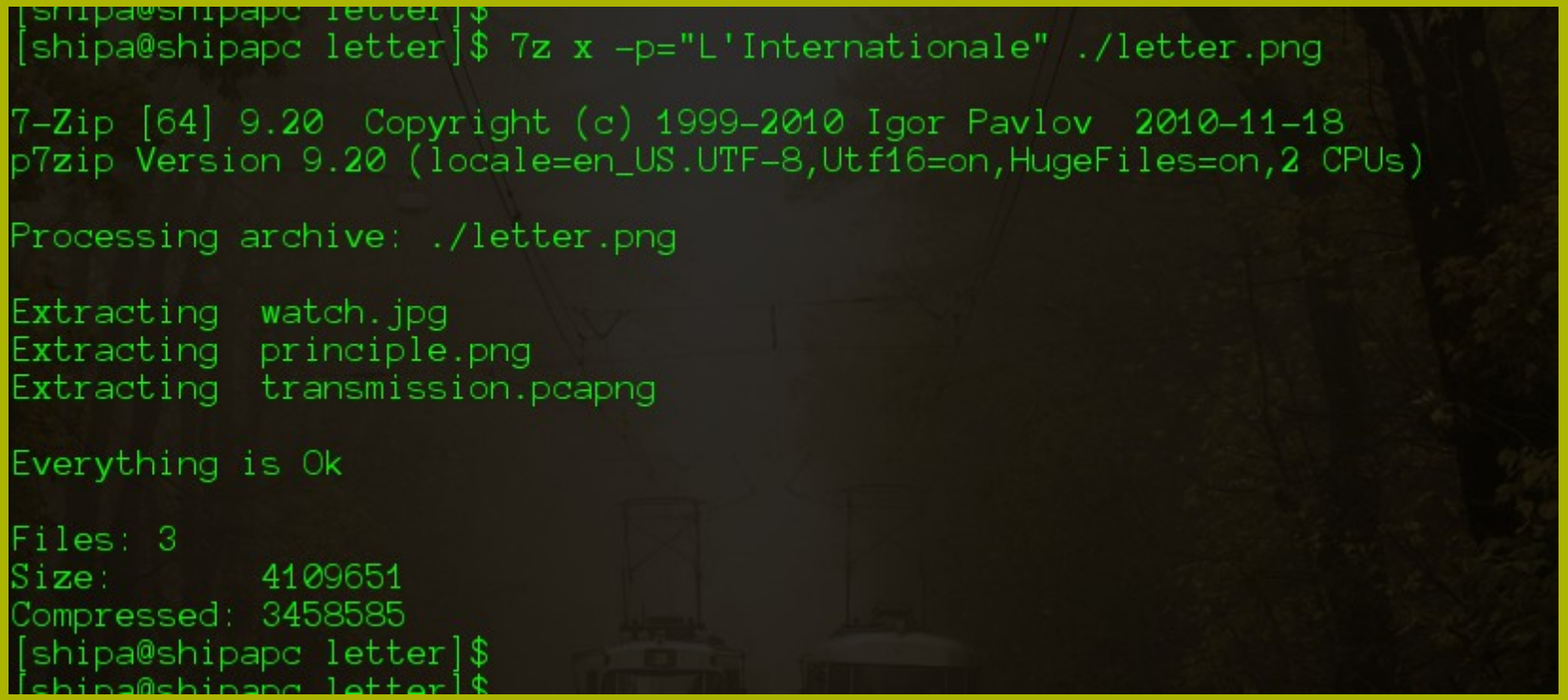
С самым лучшим коммунистическим приветом:
В. Ульянов (Ленин)

Но не все так просто!

Письмо странное -- короткий, ничего не значащий для нас текст. Но мы то все помним, как Ленин писал письма в ссылке! Молоком между строк! Поэтому применяя редактор растровой графики получаем строку "L'Internationale"



Можно попробовать сдать название гимна всех коммунистов, но ни чего не получится... Тогда обращаем внимание на большой размер картинки, понимаем, что к ней "приклеен" архив 7z. Но архив закрыт на "замок", ключ к которому мы получили на прошлом шаге.

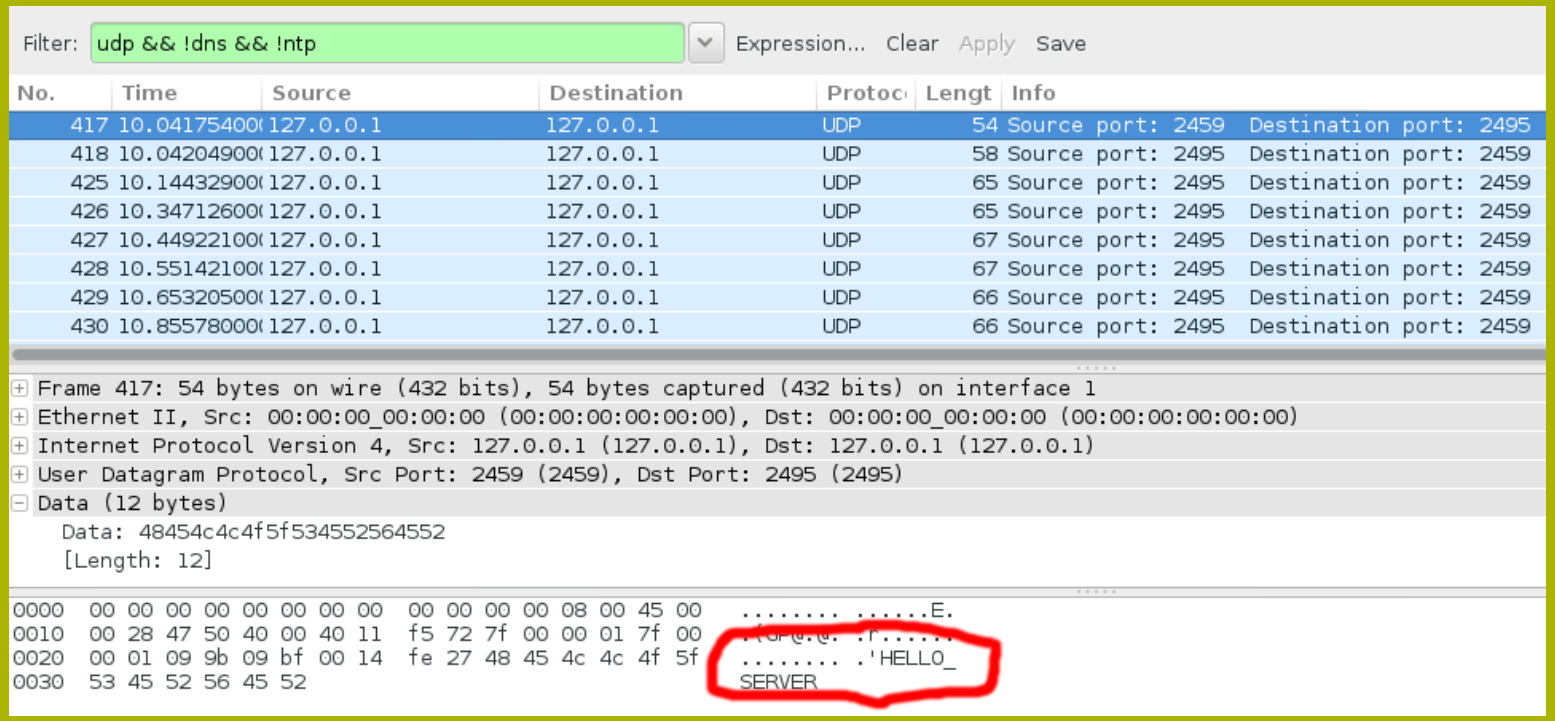


Внутри находятся 2 фотографии и перехват пакетов.

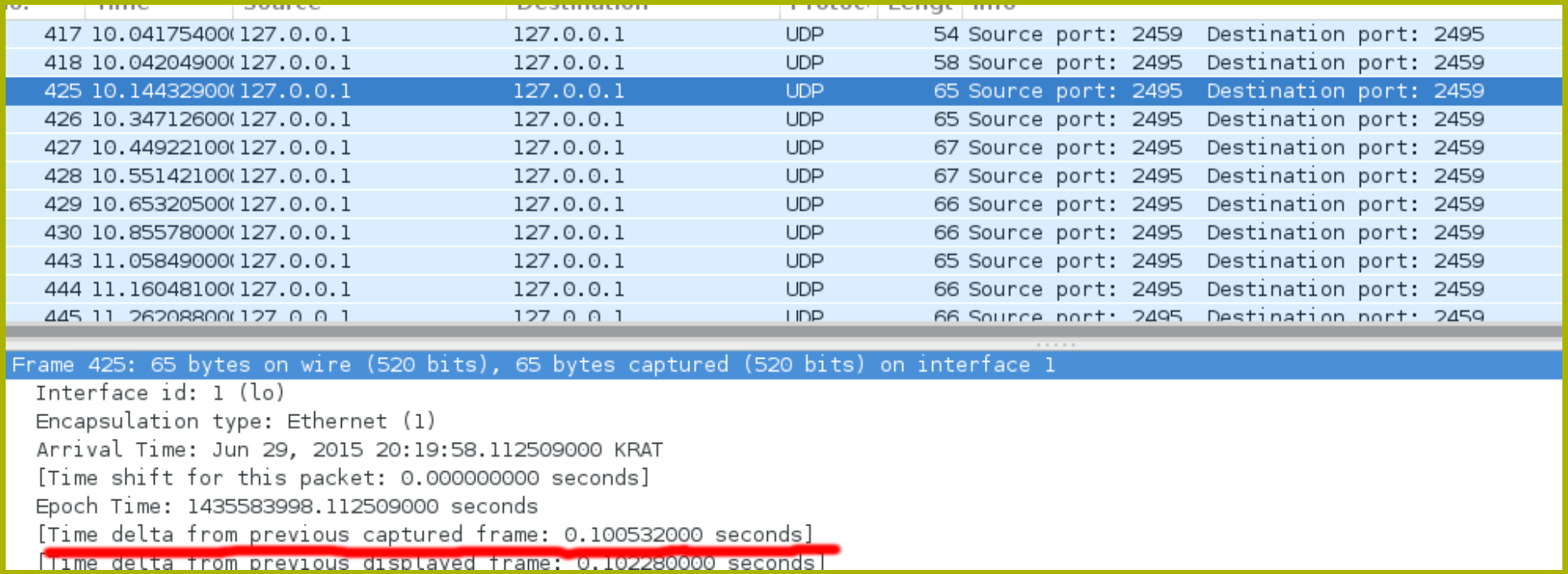
Фотография с часами (с Лубянкой :-)) намекает, что время -- очень важная часть этого задания. Timing Channel в конце концов.

Фотография с весами намекает на принцип "развесовки" временных отрезков, и на то, что ассоциировать что-то нужно только с "0" и "1".

Дамп трафика -- очевидно мусов, кроме некоторых UDP пакетов с информацией о системе. Однако, если отфильтровать в wireshark только по "UDP", захватим нужные пакеты, очевидно, что они участнику и нужны. Фильтр для wireshark: "udp && !dns && !ntp". Затем все отобраннеы пакеты сохраним в CSV-файл.



"Какие-то очень странные временные задержки между пакетами," -- подумал Ватсон, вспомнив часы с изображением Лубянки. Да! Теперь тайна раскрыта, пишем скриптик, сопостовляющий меньщей задержке "0", а большей -- "1"



Раскодировали строку

"Flag is 56FA6731"