

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!

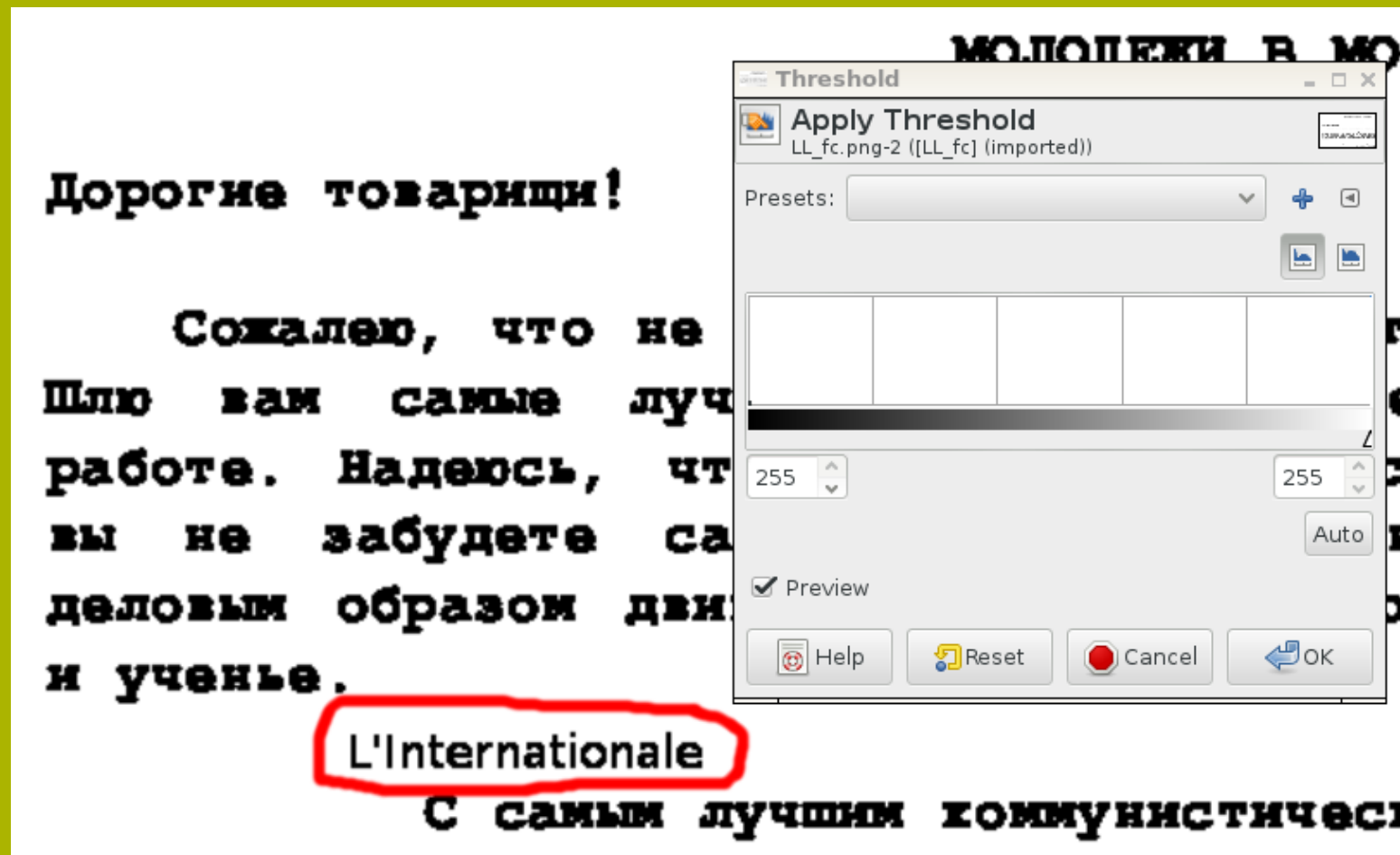
Сожалею, что не могу, приветствовать вас лично.  
Шлю вам самые лучшие пожелания успеха в вашей  
работе. Надеюсь, что, несмотря на высокое звание,  
вы не забудете самого главного — необходимости  
деловым образом двинуть вперед подготовку молодежи  
и ученье.

L'Internationale

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 картинке, понимаем, что к ней "приклеен" архив 7z. Но архив закрыт на "замок", ключ к которому мы получили на прошлом шаге.

```
[shipa@shipapc letter]$  
[shipa@shipapc letter]$ 7z x -p="L'Internationale" ./letter.png  
  
7-Zip [64] 9.20 Copyright (c) 1999-2010 Igor Pavlov 2010-11-18  
p7zip Version 9.20 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,2 CPUs)  
  
Processing archive: ./letter.png  
  
Extracting watch.jpg  
Extracting principle.png  
Extracting transmission.pcapng  
  
Everything is Ok  
  
Files: 3  
Size: 4109651  
Compressed: 3458585  
[shipa@shipapc letter]$  
[shipa@shipapc letter]$
```

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 отобранные пакеты сохраним в CSV-файл.

Filter: `udp && !dns && !ntp` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
417	10.041754000	127.0.0.1	127.0.0.1	UDP	54	Source port: 2459 Destination port: 2495
418	10.042049000	127.0.0.1	127.0.0.1	UDP	58	Source port: 2495 Destination port: 2459
425	10.144329000	127.0.0.1	127.0.0.1	UDP	65	Source port: 2495 Destination port: 2459
426	10.347126000	127.0.0.1	127.0.0.1	UDP	65	Source port: 2495 Destination port: 2459
427	10.449221000	127.0.0.1	127.0.0.1	UDP	67	Source port: 2495 Destination port: 2459
428	10.551421000	127.0.0.1	127.0.0.1	UDP	67	Source port: 2495 Destination port: 2459
429	10.653205000	127.0.0.1	127.0.0.1	UDP	66	Source port: 2495 Destination port: 2459
430	10.855780000	127.0.0.1	127.0.0.1	UDP	66	Source port: 2495 Destination port: 2459

Frame 417: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 1

Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)

User Datagram Protocol, Src Port: 2459 (2459), Dst Port: 2495 (2495)

Data (12 bytes)

Data: 48454c4c4f5f534552564552  
[Length: 12]

0000 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E.  
0010 00 28 47 50 40 00 40 11 f5 72 7f 00 00 01 7f 00 .....f.....  
0020 00 01 09 9b 09 bf 00 14 fe 27 48 45 4c 4c 4f 5f ..... 'HELLO\_  
0030 53 45 52 56 45 52 .....SERVER

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

No.	Time	Source	Destination	Protocol	Length	Info
417	10.041754000	127.0.0.1	127.0.0.1	UDP	54	Source port: 2459 Destination port: 2495
418	10.042049000	127.0.0.1	127.0.0.1	UDP	58	Source port: 2495 Destination port: 2459
425	10.144329000	127.0.0.1	127.0.0.1	UDP	65	Source port: 2495 Destination port: 2459
426	10.347126000	127.0.0.1	127.0.0.1	UDP	65	Source port: 2495 Destination port: 2459
427	10.449221000	127.0.0.1	127.0.0.1	UDP	67	Source port: 2495 Destination port: 2459
428	10.551421000	127.0.0.1	127.0.0.1	UDP	67	Source port: 2495 Destination port: 2459
429	10.653205000	127.0.0.1	127.0.0.1	UDP	66	Source port: 2495 Destination port: 2459
430	10.855780000	127.0.0.1	127.0.0.1	UDP	66	Source port: 2495 Destination port: 2459
443	11.058490000	127.0.0.1	127.0.0.1	UDP	65	Source port: 2495 Destination port: 2459
444	11.160481000	127.0.0.1	127.0.0.1	UDP	66	Source port: 2495 Destination port: 2459
445	11.262088000	127.0.0.1	127.0.0.1	UDP	66	Source port: 2495 Destination port: 2459

.....

Frame 425: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface 1

Interface id: 1 (lo)

Encapsulation type: Ethernet (1)

Arrival Time: Jun 29, 2015 20:19:58.112509000 KRAT

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1435583998.112509000 seconds

[Time delta from previous captured frame: 0.100532000 seconds]

[Time delta from previous displayed frame: 0.102280000 seconds]



Раскодировали строку

"Flag is 56FA6731"

```
0.403269000000002
0.402949000000003
0.102923999999994
0.102189000000003
0.102156999999998
0.403088000000004
0100011001101100011000010110011100100000011010
0001
Flag is 56FA6731
[Shippe@Shippe materials]$
```