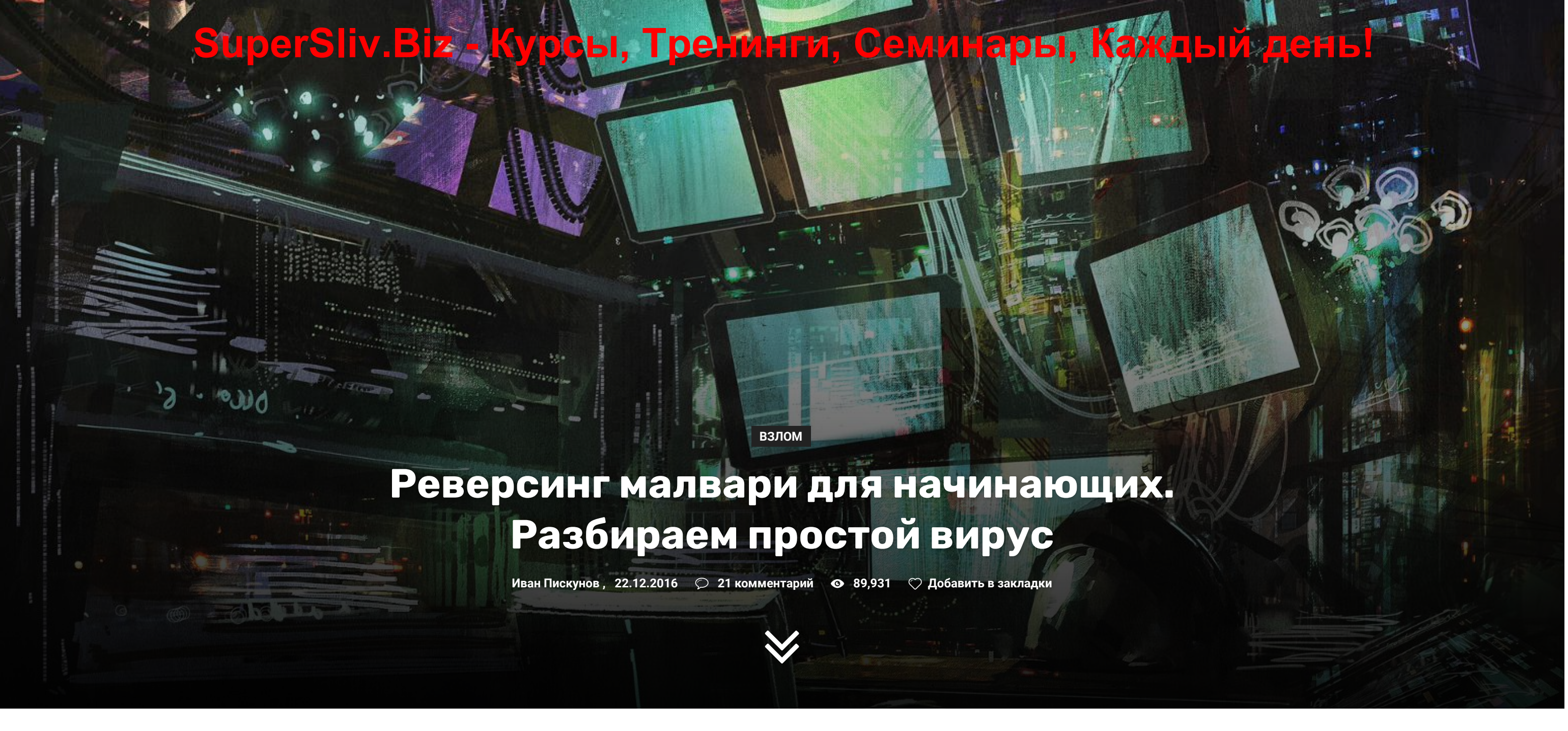


Реверсинг малвари для начинающих. Разбираем простой вирус

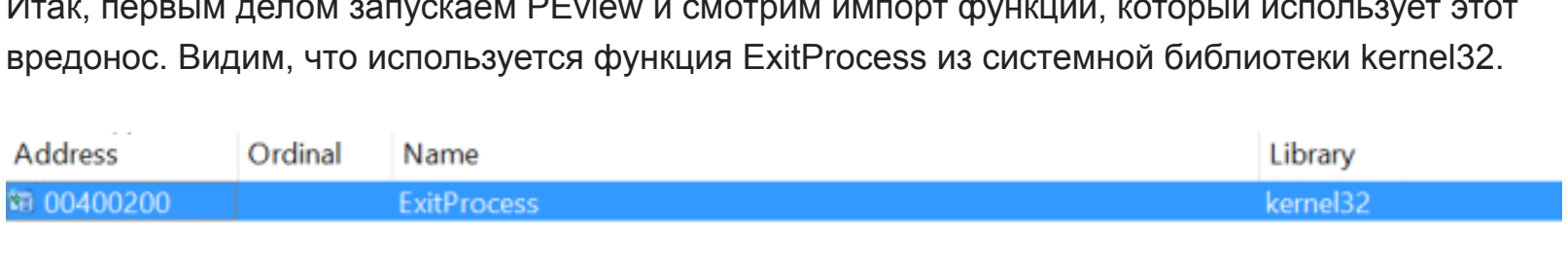
Содержание статьи

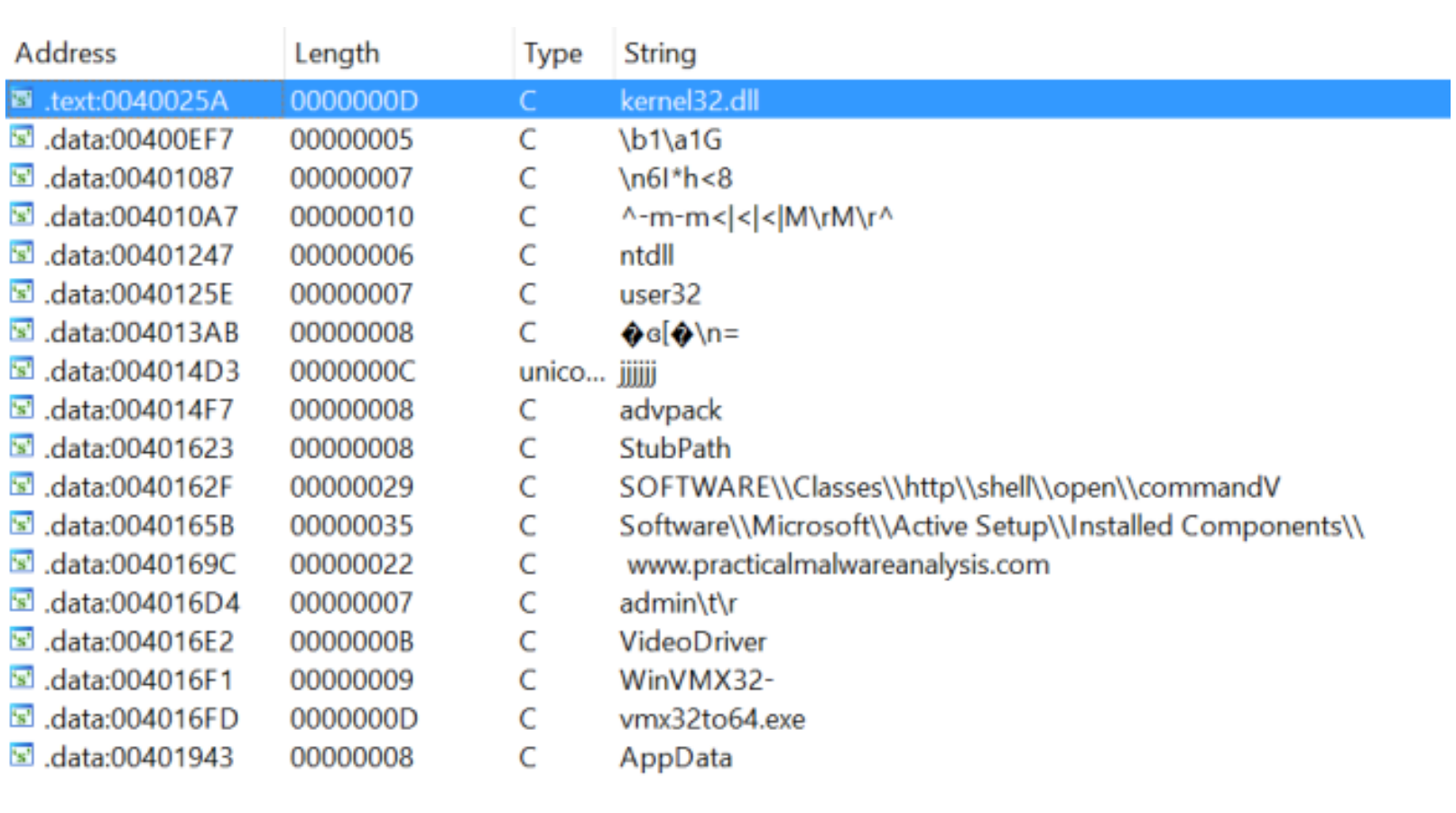
Подготовка рабочего окружения

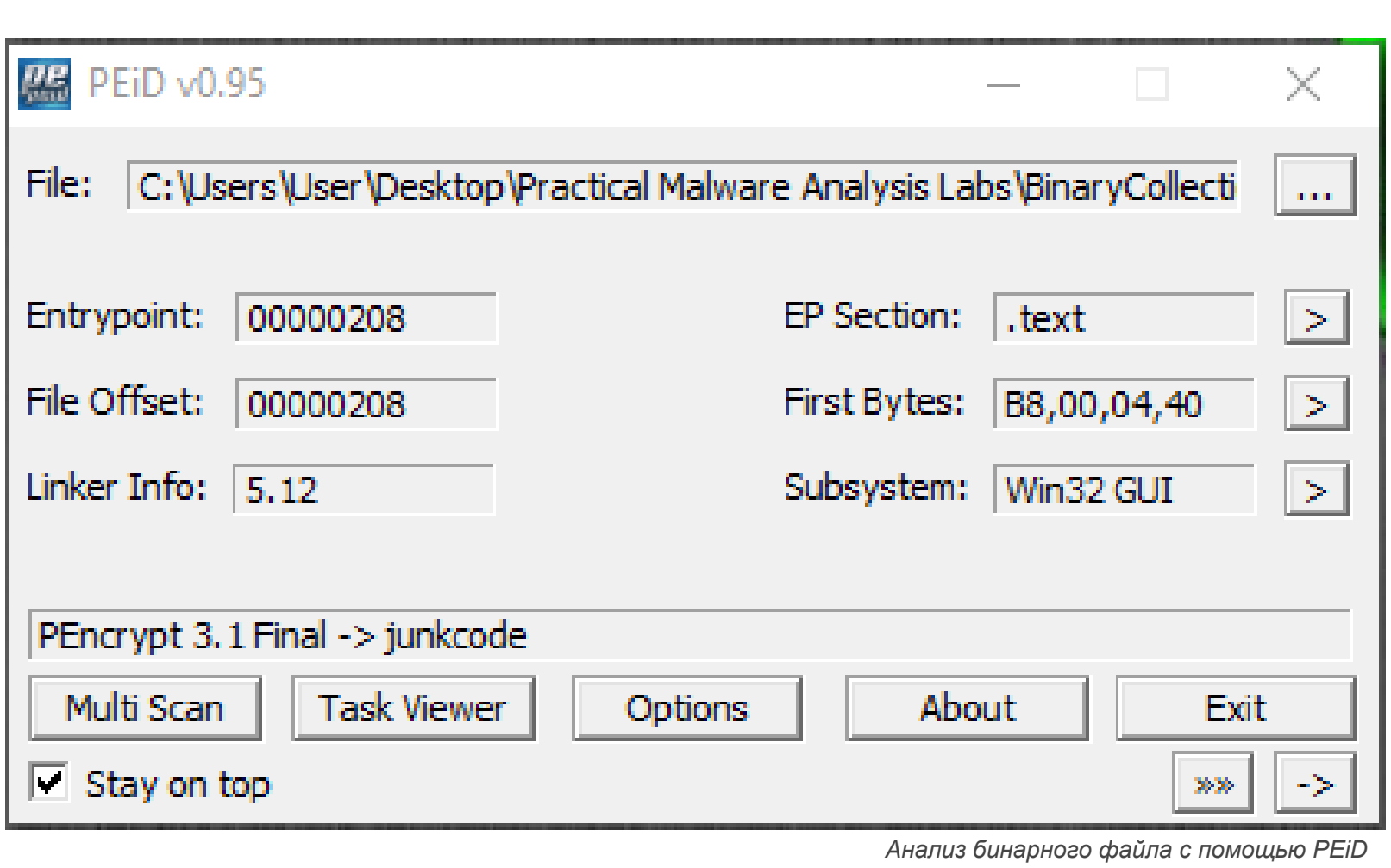
Анализ семпла Lab01: динамический анализ

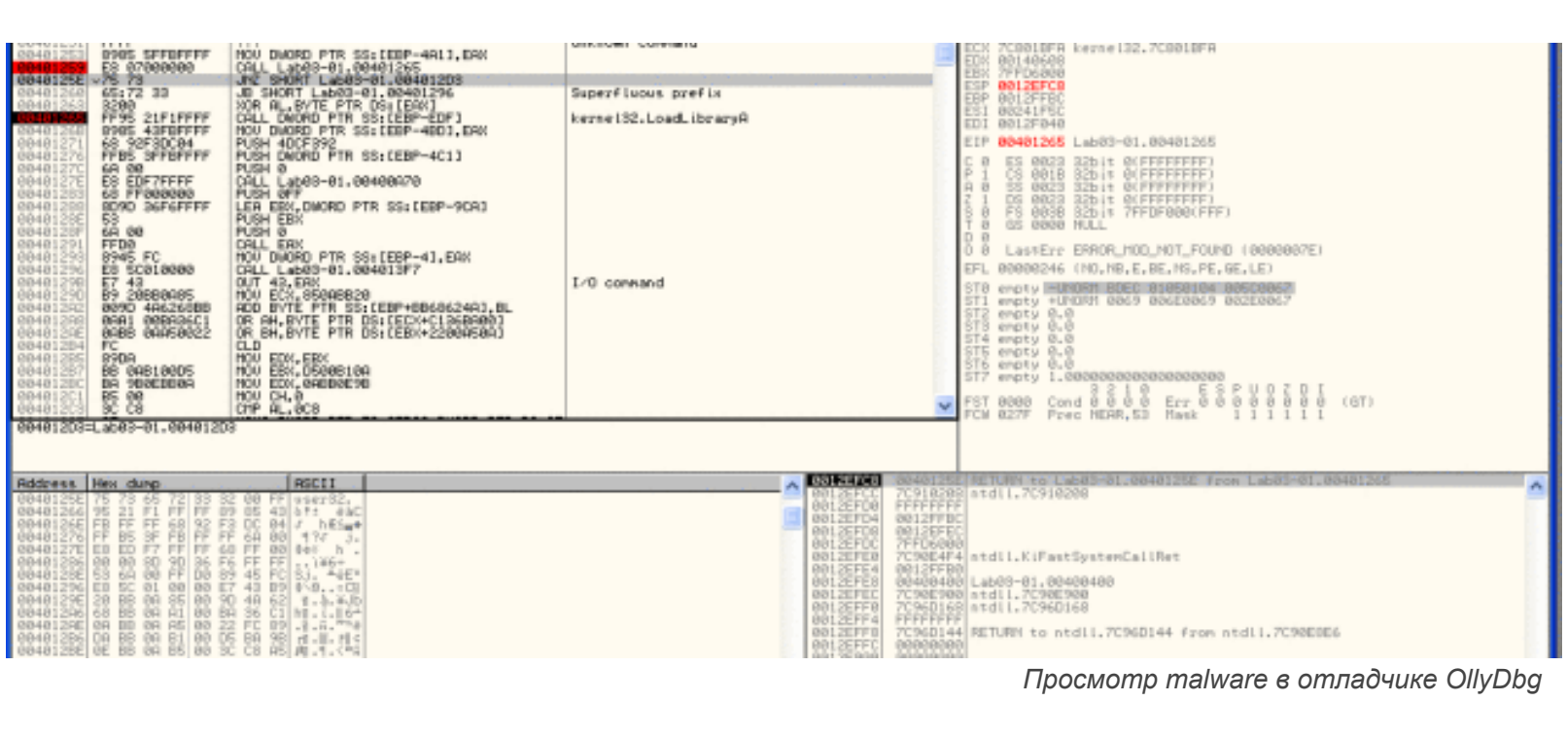
- IDA Pro,
- PEiD,
- RegShot,
- Procmon,
- Wireshark,
- Process Explorer,
- OllyDbg.

WARNING

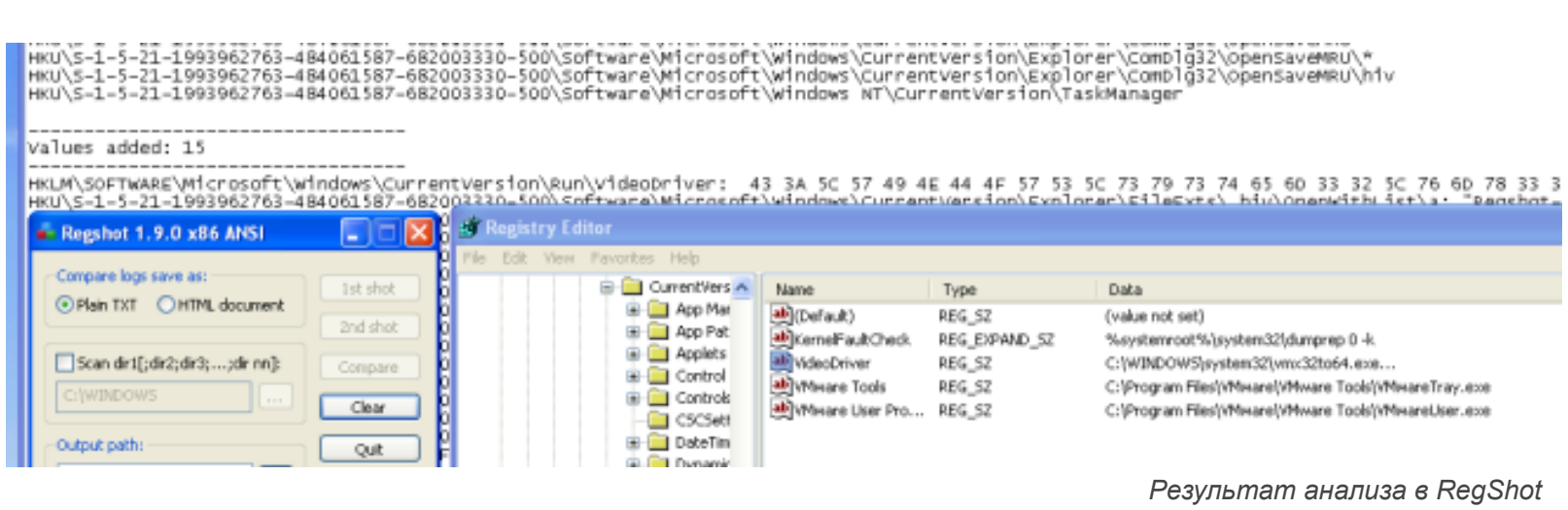




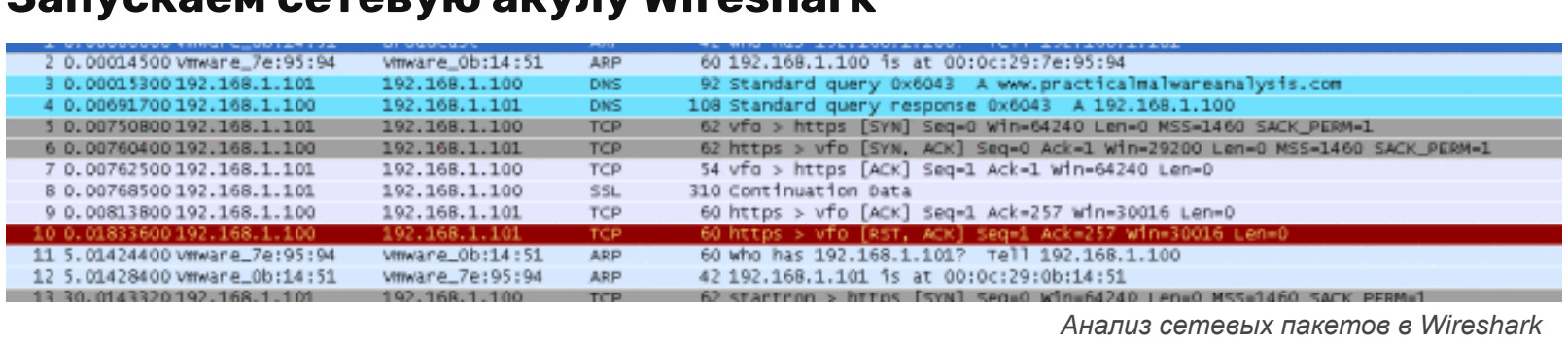


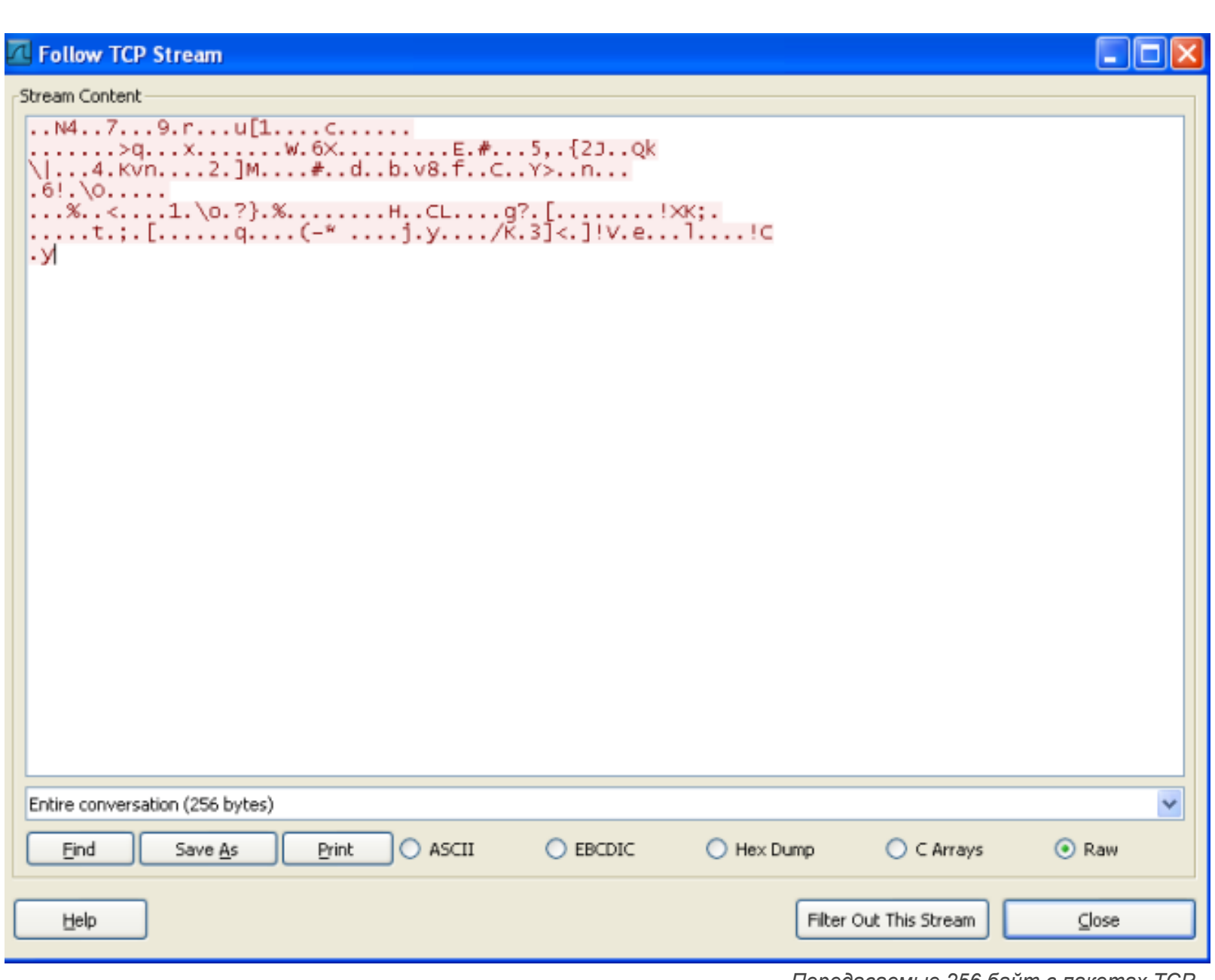


Продолжаем исследование. Смотрим реестр

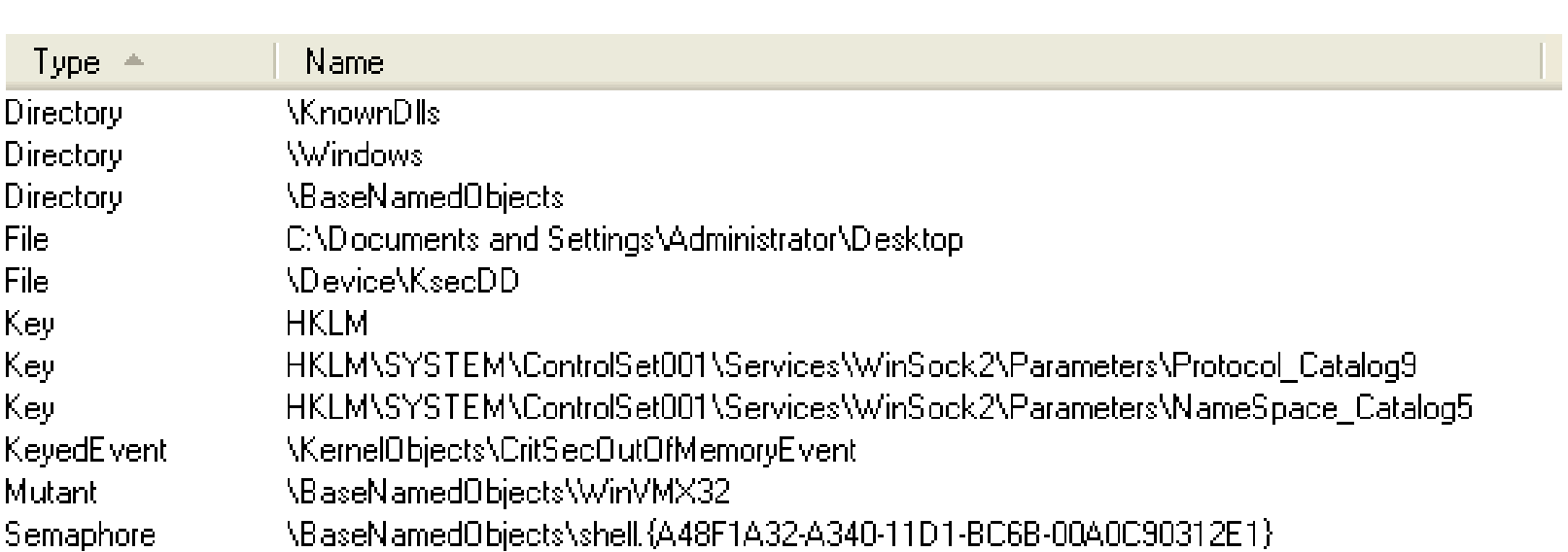


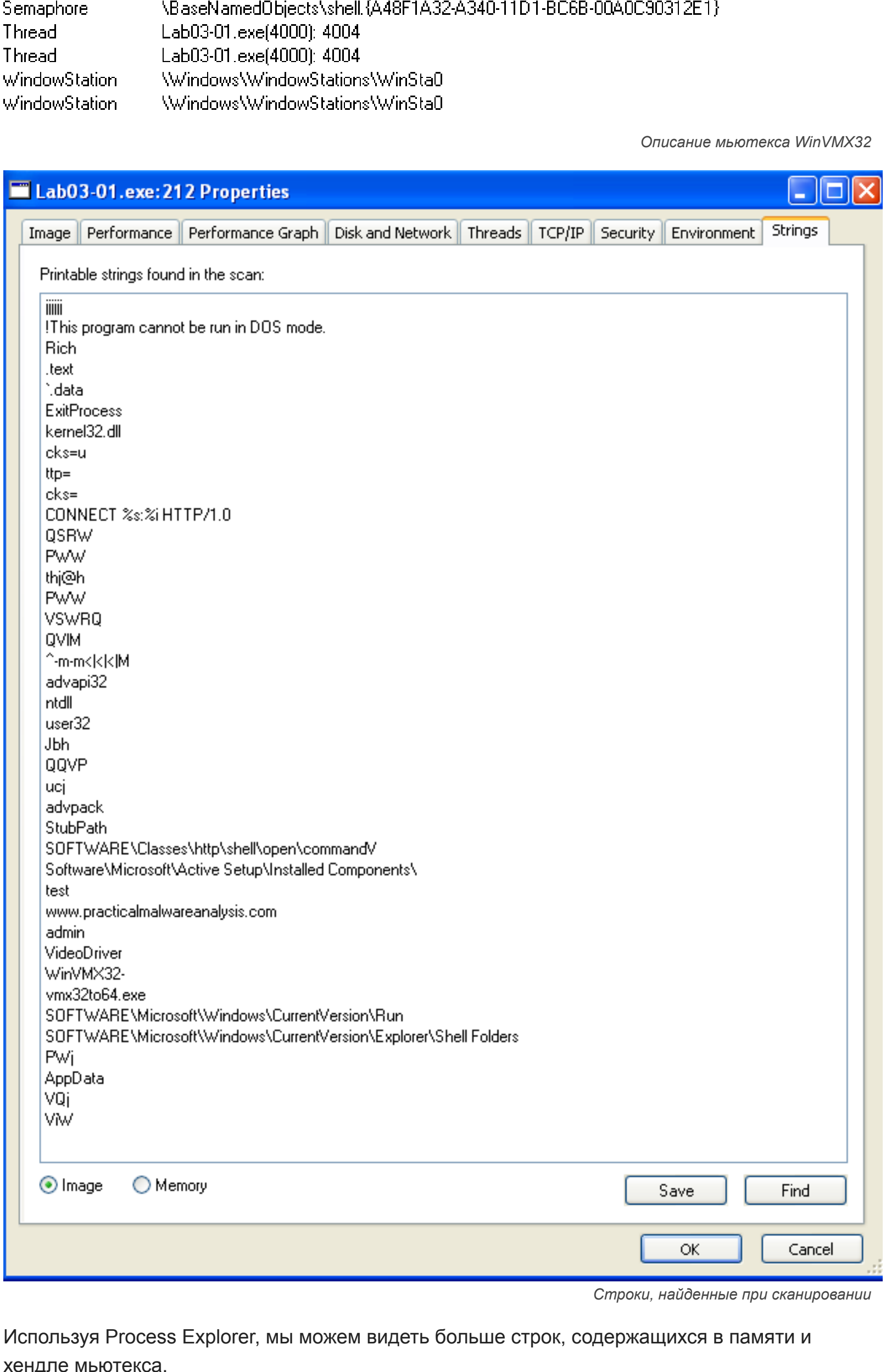
Запускаем сетевую акулу Wireshark

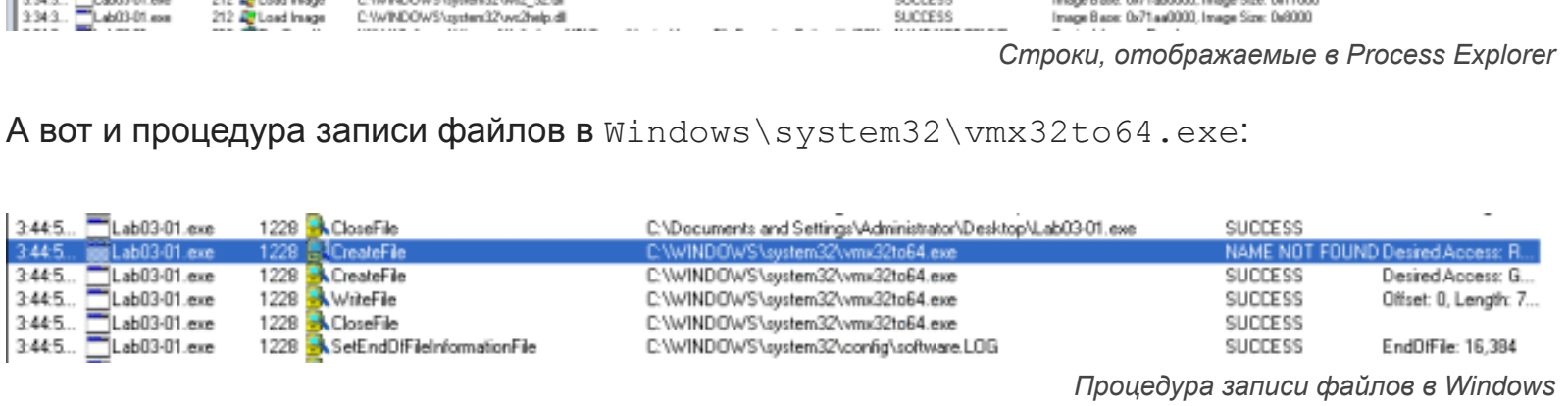




Что нам покажет Process Explorer?

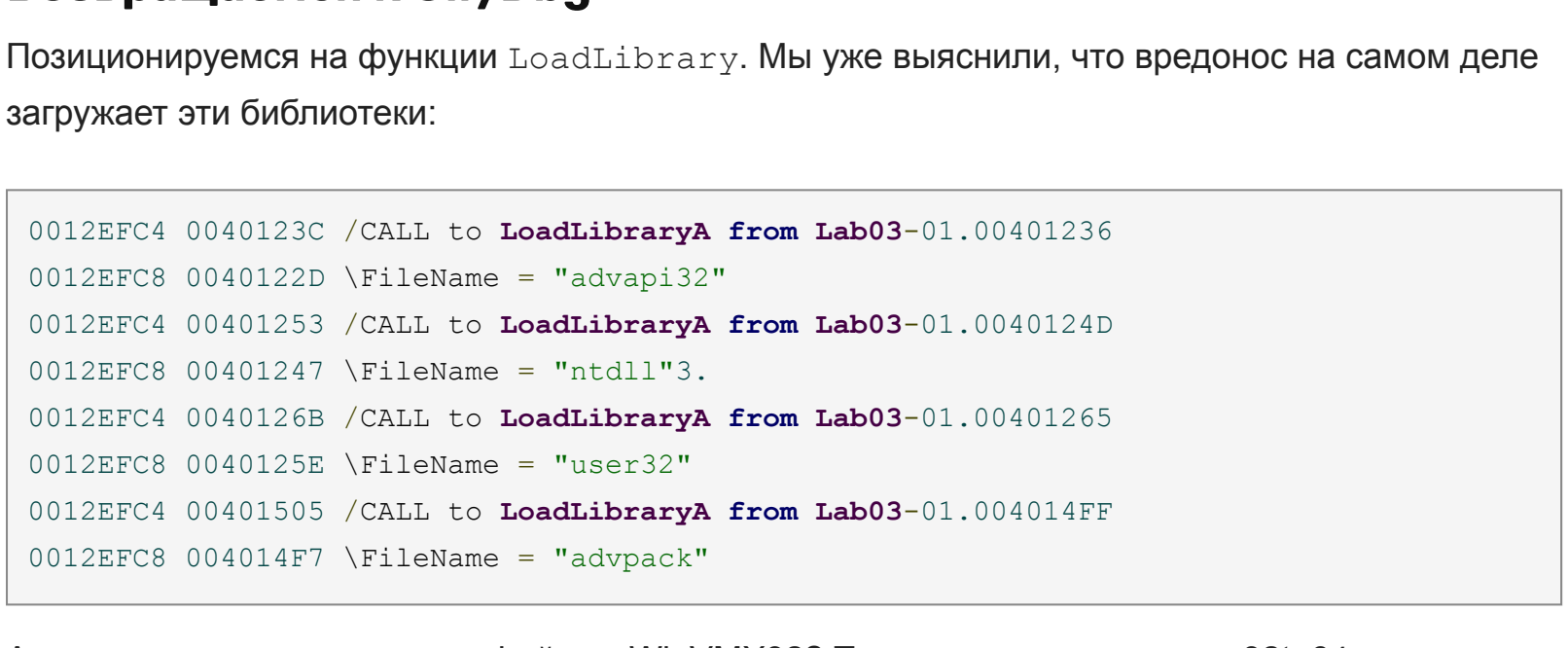


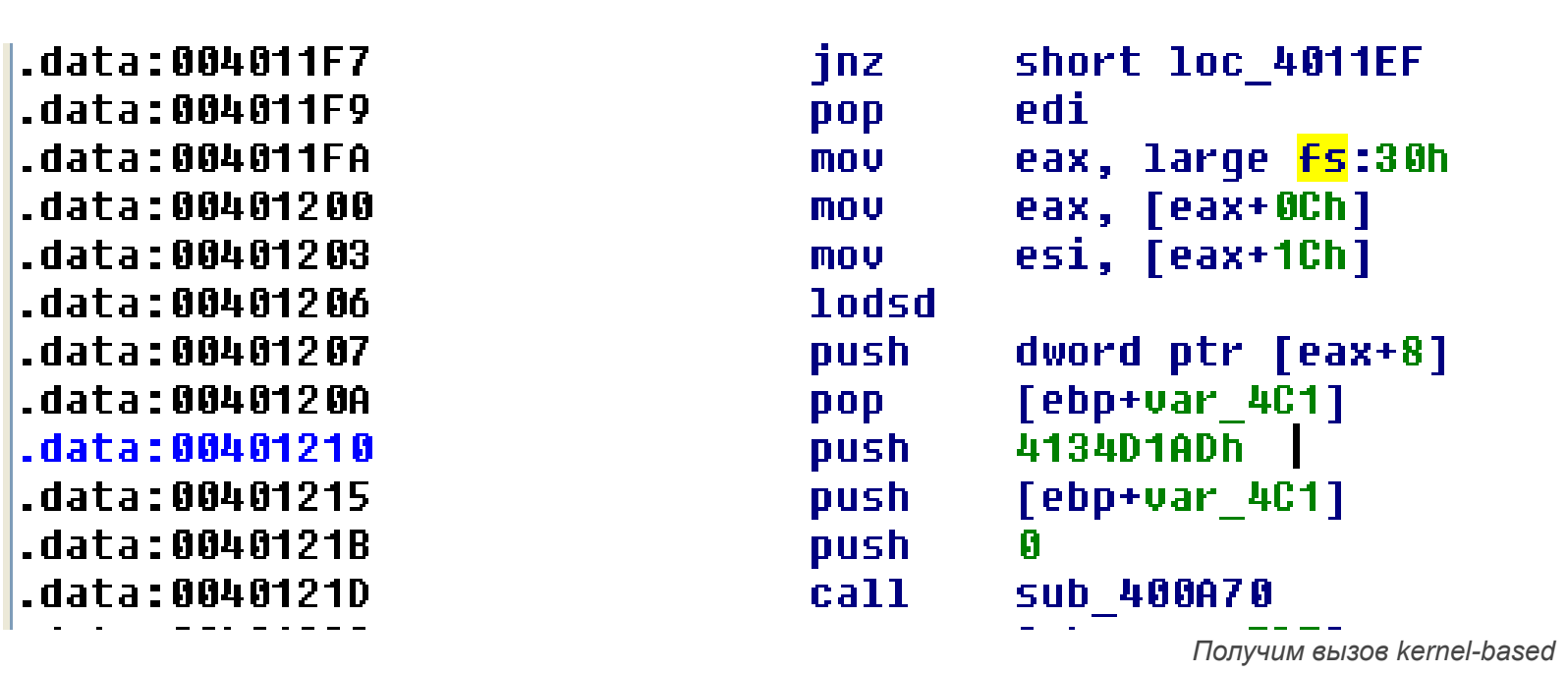


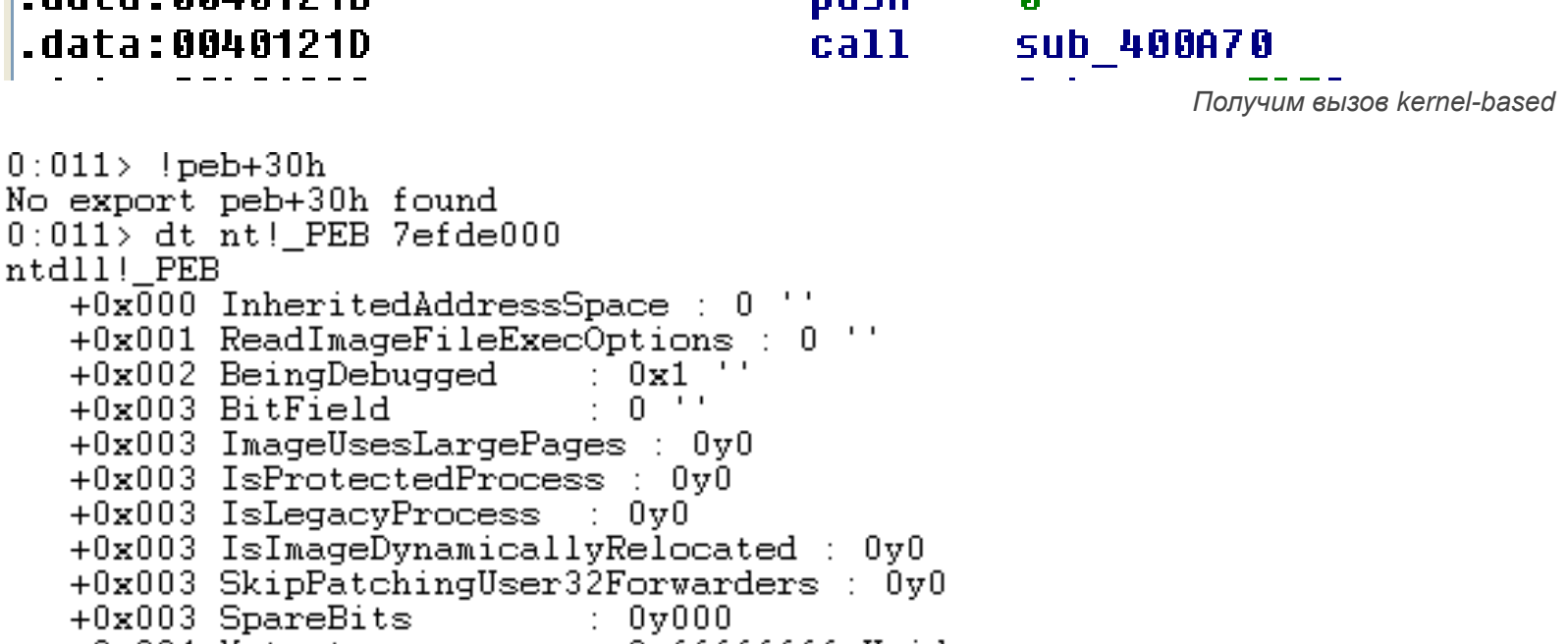


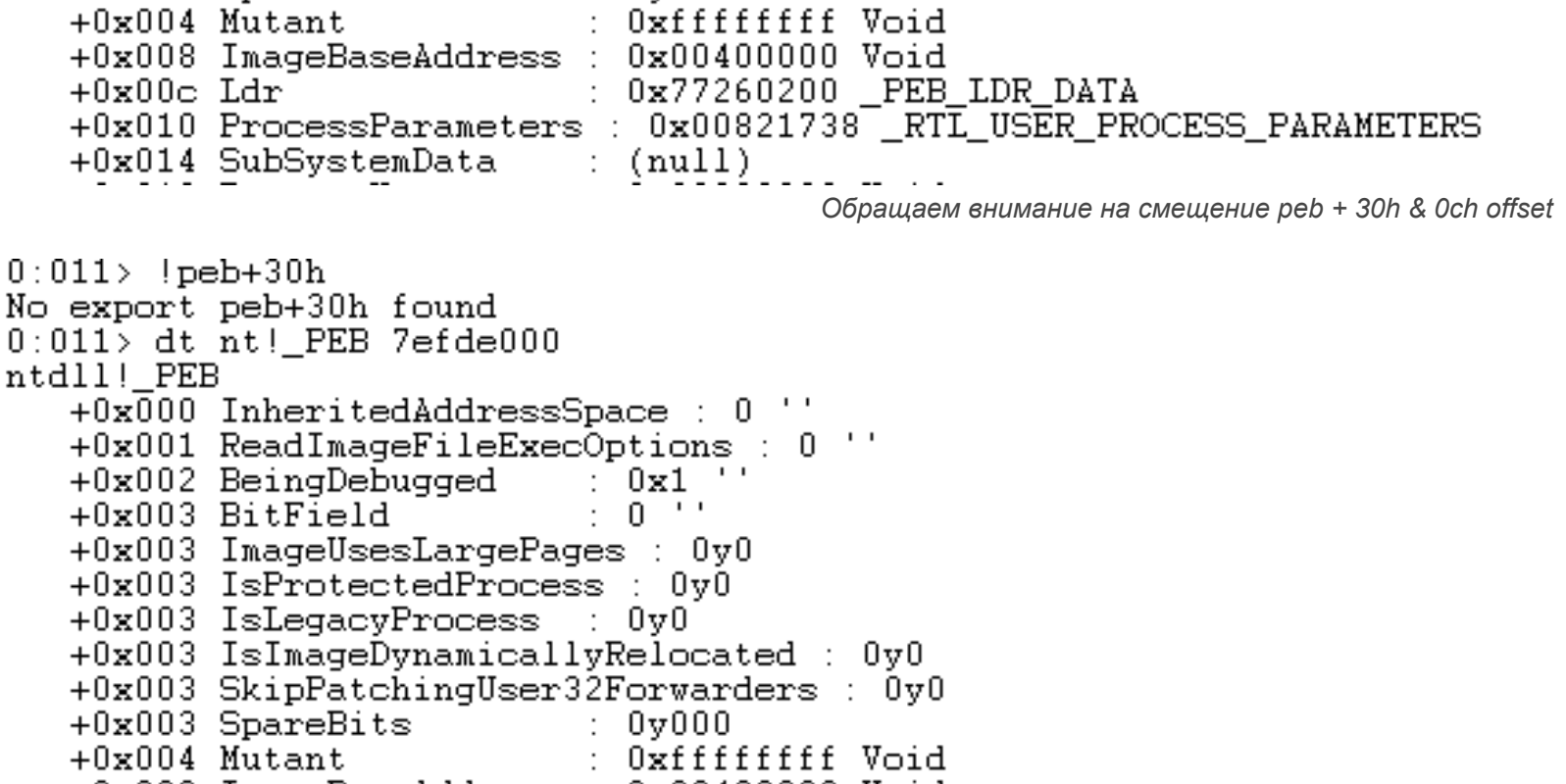
WARNING

Возвращаемся к OllyDbg









INFO

Заключение