# Искусство удаленной отладки: готовим инструментарий для работы с ядром и вирусами

Автор: Дмитрий Оксенчук, ООО «Лаборатория Касперского»

## Содержание статьи

1. Установка и настройка виртуальной машины
2. Удаленная отладка в Microsoft Visual Studio
3. Удаленная отладка в IDA Starter
4. Настройка WinDbg/VirtualKD
5. Анализ закрытого дампа при помощи WinDbg
6. Заключение

Необходимость в отладке программ, запущенных внутри виртуальной машины, может возникнуть, когда вы пишете клиентский код, удаленно или на виртуальной машине, отладчик для которой вы не можете запустить, или когда вы пишете вредоносное ПО, которое использует инструкции, которые поддерживает лишь один процессор, или в каждом втором вирусе. Быть непросто, так что данной посмотрим, какими они бывают и как с ними обращаться.

### Установка и настройка виртуальной машины

Чтобы начать наше экспериментировать, необходимо установить свою виртуальную среду. Кто-то предпочитает VMware, кто-то VirtualBox, кто-то Hyper-V, но мы выберем Virtual PC, поскольку в дальнейшем нам понадобится удаленная отладка ядром операционных систем и работа с дампами. Virtual PC, к сожалению, не поддерживает подключение к виртуальным машинам по сети, поэтому нам потребуется виртуальная машина с гостевой ОС на основе Windows. Также нам понадобится виртуальная машина с гостевой ОС на основе Linux. Также следует выбрать тип виртуализируемых ВМ, а он есть. Это решается для совместимости с различными операционными системами, которые мы будем использовать.

Параметры
Имя виртуальной машины: Win7x64
Расположение: C:\Users\Public\Documents\Virtual Machines\Win7x64\
Сохранять файлы виртуальных жестких дисков в расположении по умолчанию
Сохранять файлы виртуальных жестких дисков в следующем расположении:
Сохранять изменения в виртуальных жестких дисках по завершении работы виртуальной машины