открытом доступе. Тем, кто хочет понять концептуальные основы анализа и общую методологию исследования к прочтению обязательно!

2. Перевод на русский описанного выше документа, представленный Prosper-H, coldfire, ximera. Подойдет тем, кто пока что плохо понимает английский.
3. Онлайн-курс Free Malware Analysis Training Class from Cybrary, состоящий из семи обучающих модулей, построенных по принципу от простого к сложному, включает в себя все основные темы: статический и динамический анализ, расширенный анализ, распаковка и практические лабораторные работы. Полный курс длится девять часов, после него можно сдать сертификационный экзамен.
4. Cheat Sheet for Analyzing Malicious Software от Ленни Зельцера (Lenny Zeltser) — несколько небольших шпаргалок по анализу вредоносного ПО.

Наиболее интересные платные обучающие курсы

1. Платный курс от университета SANS под названием FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques. Курс рассчитан на четыре месяца обучения, состоит из шести обучающих модулей, каждый подкреплен практическими работами. Затрагиваются темы: компьютерная форензика, первичный и детальный анализ вредоносного ПО, использование утилит мониторинга сети, дизассемблера, отладчика и многих других полезных инструментов. Курс обойдется в кругленькую сумму от 5000 USD.
2. Платный обучающий курс от компании FireEye рассказывает с самых основ о техниках быстрого и продвинутого анализа малвари. На сайте можно ознакомиться с программой курса. Сам курс рассчитан как на новичков, так и на более продвинутых слушателей, длится от двух до четырех дней и включает в себя теоретический и практически материал.
3. Еще один платный курс от компании ThreatTrack демонстрирует возможности анализа малвари с использованием специально разработанного компанией инструмента — песочницы **ThreatAnalyzer**. Для зарегистрированных пользователей существует возможность попробовать 30-дневную триал-версию.

Форумы

1. Tuts 4 You — англоязычный форум, один из самых популярных и авторитетных среди подобных, целиком посвящен вопросам реверсинга ПО, в том числе анализу вредоносов. Имеется и русскоязычная ветка, где обитает большое количество соотечественников, готовых поделиться опытом и образцами.
2. eXeL@B — крупнейший форум в русскоязычном сегменте сети, также целиком сфокусированный на изучении и анализе программ, реверсинге и всем, что с этим связано.

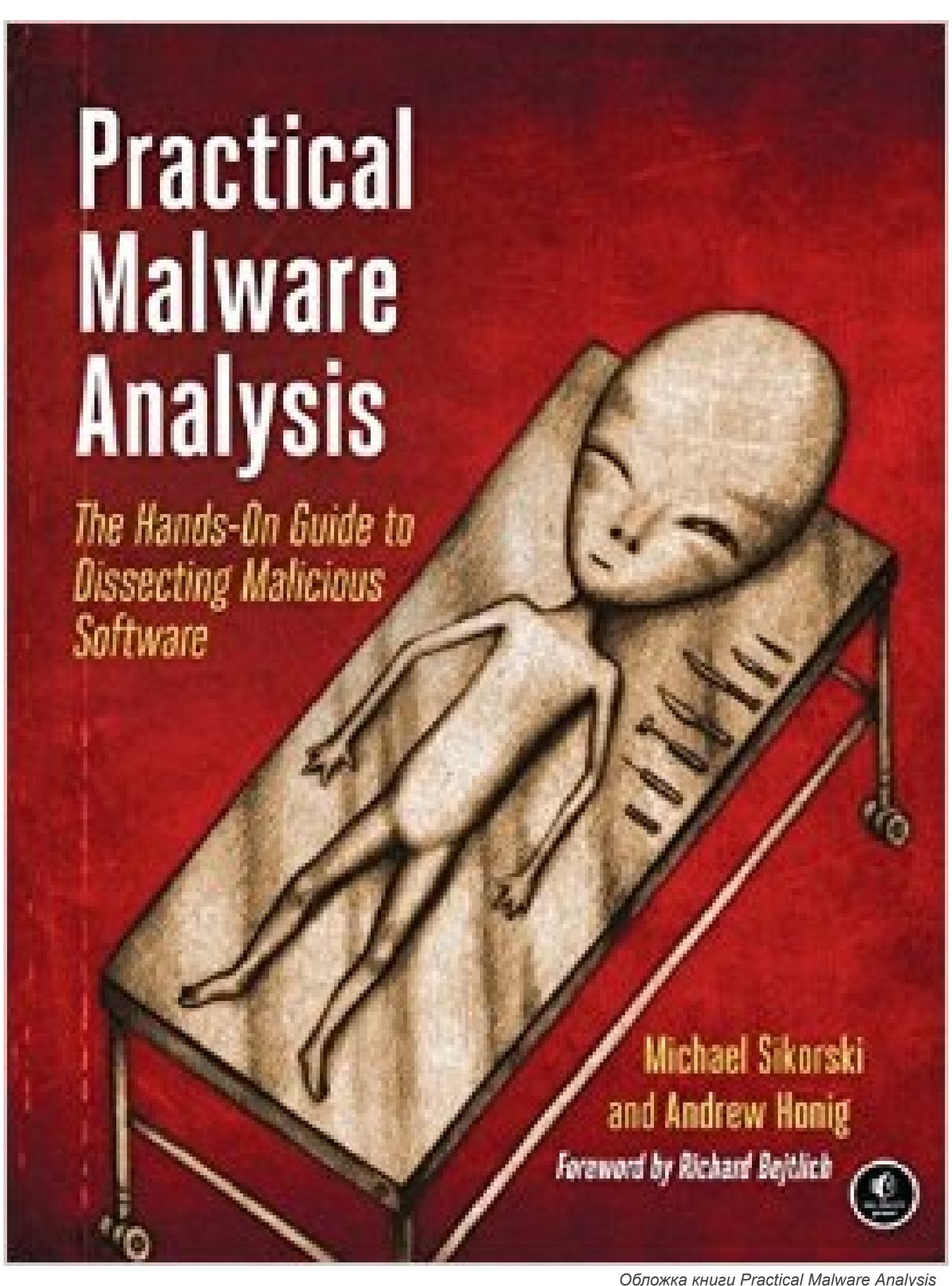
Авторские сайты и блоги

1. Блог Роберта Галвана, посвященный вопросам безопасности и, в частности, исследованию малвари. Автор разместил несколько статей с описанием анализа.
2. Авторский сайт Мэтта Бриггса и Франка Поца (Matt Briggs & Frank Poz), целиком посвященный изучению реверсинга вредоносного ПО. На сайте есть цикл лекций по двухдневному тренингу. Для скачивания доступны лекционные материалы, презентации и образцы исследуемых объектов.

Книги

Книги по исследованию программного обеспечения и обратной разработке — литература весьма специфическая и узкоспециализированная. Поэтому их издано очень мало, и русскоязычных (переводных) среди них единицы. Однако, на радость нам, есть достойные экземпляры.

1. **Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software**.

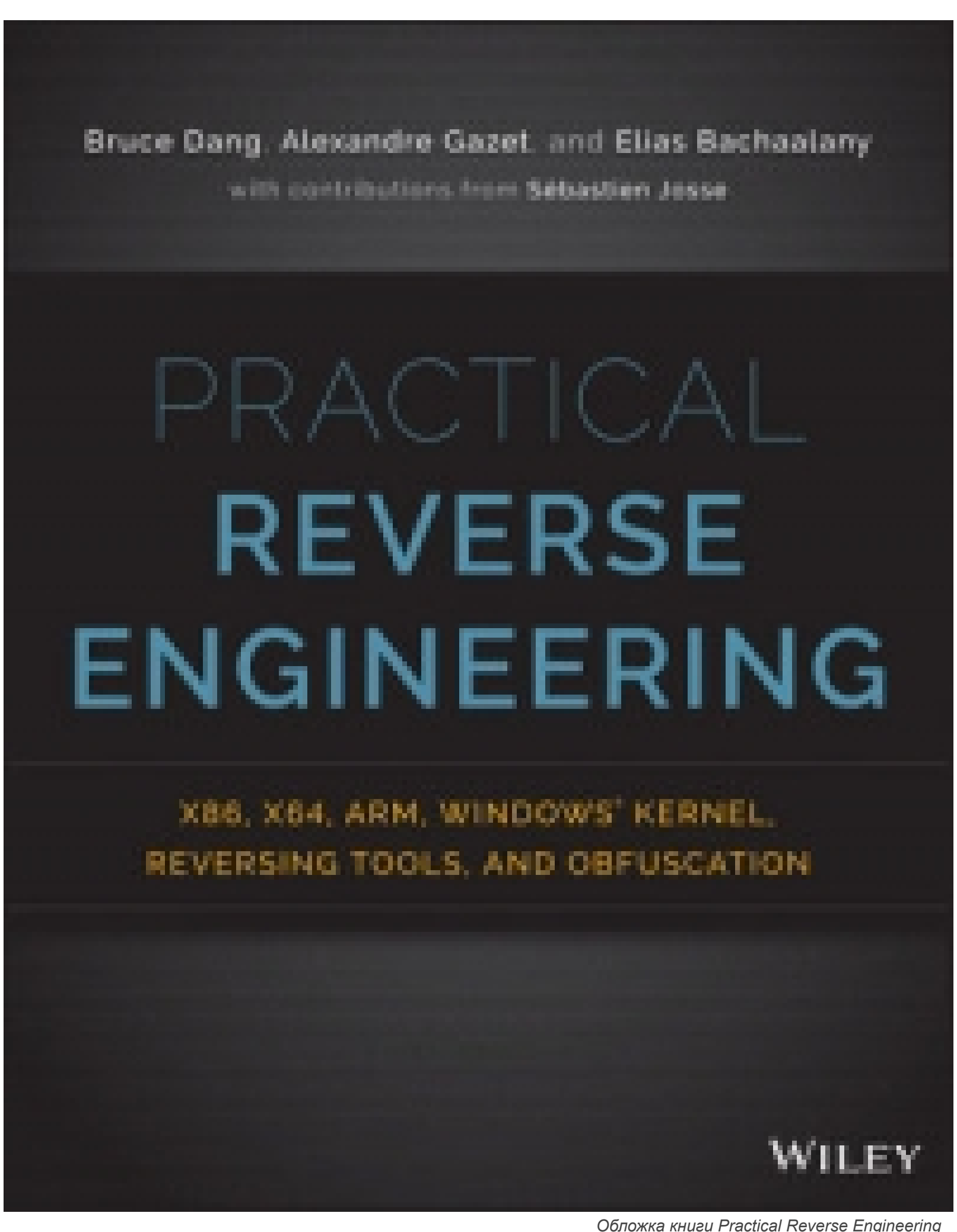


Обложка книги Practical Malware Analysis

Книга Practical Malware Analysis представляет собой некое подобие учебного пособия, где подробно описываются рабочие инструменты и техники реверсинга, а в конце почти всех глав приводится список лабораторных работ к изложенному материалу. С каждой новой главой читатель узнает все больше и закрепляет знания на все усложняющихся лабораторных работах.

Доставшаяся мне книга была без CD с лабами, но, как заверяет описание, их можно найти на официальном сайте книги.

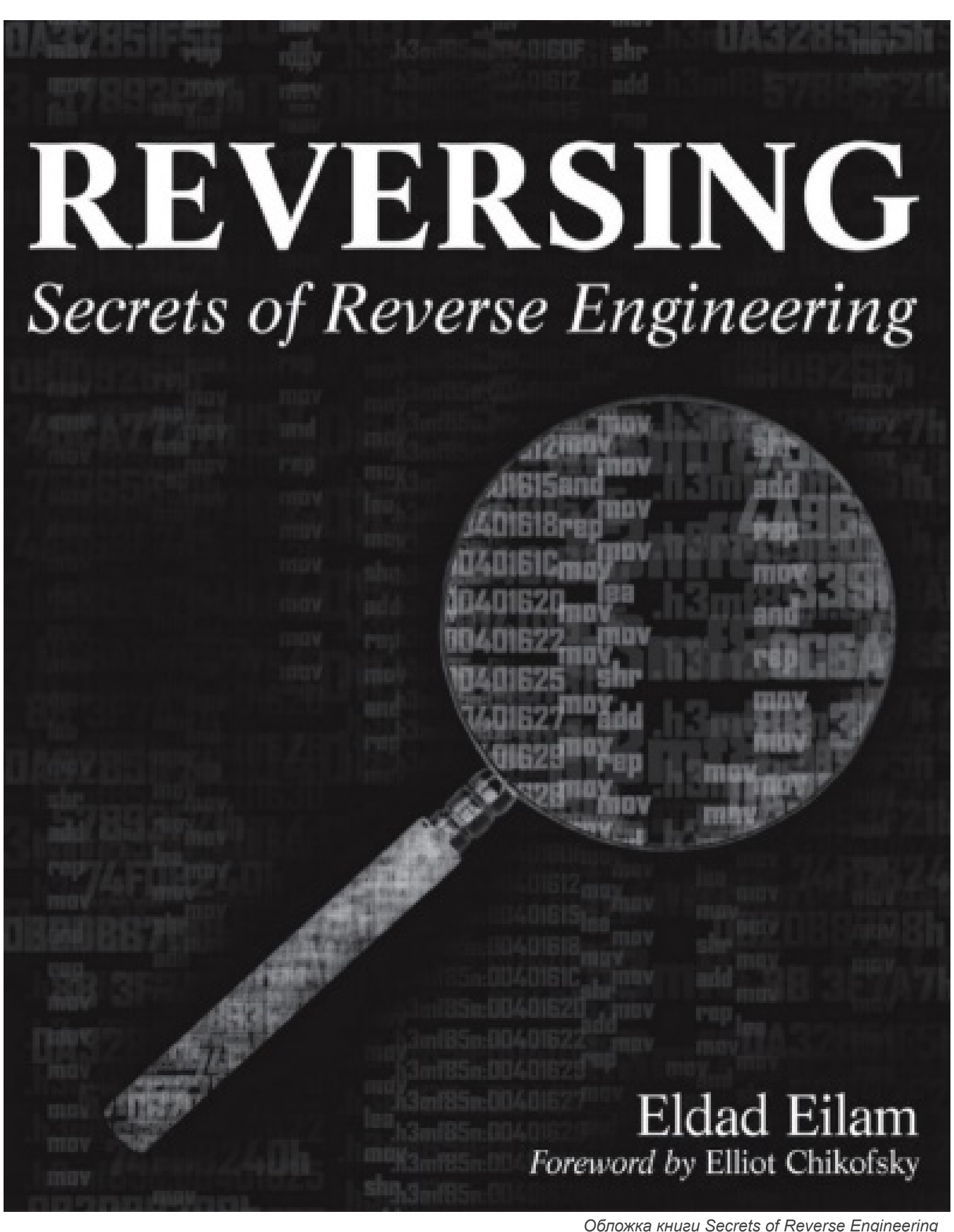
1. **Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation**.



Обложка книги Practical Reverse Engineering

Тоже весьма интересная книга с упором на практический реверс-инжиниринг, нацеленная прежде всего на аналитиков, инженеров по безопасности и системных программистов. В книге рассматриваются архитектуры x86, x64 и ARM, а также детально режим ядра Windows, технологии rootkit, методы обфускации, антиотладочные трюки. Текст насыщен практическими упражнениями и реальными примерами. Книга больше касается именно реверсинга софта, чем анализа малвари, но однозначно пригодится!

1. **Reversing: Secrets of Reverse Engineering**.



Обложка книги Secrets of Reverse Engineering

Книга очень похожа на предыдущую — это тоже практическое руководство по реверсингу программного обеспечения. Каждая глава начинается с теории, объяснения тех или иных принципов, подходов, далее демонстрируются примеры практических действий. Иллюстрируются технологии дисассемблирования, разбора машинных инструкций на языке ассемблера. Затронуты вопросы взаимодействия анализируемой программы со сторонними библиотеками. В общем, отличное чтиво!

1. **Reverse Engineering for Beginners free book, Денис Юричев**.

Обложка книги Reverse Engineering for Beginners

Книга нашего соотечественника Дениса Юричева (сайт автора). Очень полезное руководство по реверсингу для начинающих на русском языке. Настоящий кладезь знаний, почти тысяча страниц подробнейшего разбора кода, реальных примеров «вскрытия», особенностей отладки в той или иной ОС, пошаговые руководства к действию. А также упражнения и задачи, которые доступны на сайте.

Полную подборку рекомендуемой литературы можно посмотреть здесь.

Сертификация Certified Reverse Engineering Analyst

Точно так же, как для этичных хакеров есть сертификация **CEH** от организации Eccouncil, так и для исследователей ПО есть аналогичная Certified Reverse Engineering Analyst (**CREA**). Согласно описанию, представленному на официальном сайте организации IACRB, слушатель должен пройти двухмесячный курс обучения, после чего необходимо сдать сертификационный экзамен, набрав минимум 210 баллов из возможных 300 (70%) для получения сертификата. На сайте размещена подробная программа курса и продемонстрированы несколько практических работ, которые выполняются на курсе. Более подробно о сертификации CREA можно узнать на официальной страничке.

Инструменты и другой софт для исследователя

1. На сайте команды The Legend Of Random размещено много материалов по реверсингу ПО. Отдельная страничка посвящена инструментам и вспомогательному софту, необходимому для проведения анализа. Все рассматриваемые инструменты доступны для свободного скачивания.
2. Компания AlienVault разместила на своем сайте страничку с описанием софта, используемого в нашем деле. Приведено подробное описание к каждому инструменту, скриншот и ссылка на источник, откуда программу можно загрузить.
3. Файловый архив eXeL@B, наверное, самый большой и полный набор крекерских инструментов из тех, что я когда-либо встречал. Более того, каждую программу, документацию, плагины и дополнения можно свободно скачать с сайта лаборатории. Для тех, у кого такая возможность отсутствует, есть вариант заказать копию сайта на DVD.

WARNING

Будь осторожен при скачивании и распаковке архивов с malware на компьютер. Все исследования выполняй только в изолированной виртуальной среде! Не выполняй действий, в которых на 100% не уверен!

Репозитории и базы данных малвари

Настало время поговорить о хранилищах, откуда можно скачать малварь или отдельные семплы для практических занятий. Помни, при скачивании твой антивирус, скорее всего, будет блокировать загрузку, поэтому позаботься об этом заранее. И конечно же, будь осторожен, чтобы случайно не заразить свой компьютер.

1. Contagio Malware Dump — коллекция последних образцов вредоносов.
2. Das Malwerk — свежие наборы вредоносов на любой вкус.
3. KernelMode.info — репозиторий, заточенный под Win32 и rootkit Windows.
4. DamageLab.in — специализированный форум, где можно найти много полезного, в том числе выкладываемые исследователями распакованные и дешифрованные семплы, методики и рекомендации по их анализу.
5. MalwareBlacklist — ежедневно обновляемая доска blacklisted URLs, зараженных малварью.
6. Open Malware — база данных с возможностью поиска вредоносного файла по имени или хешу MD5, SHA-1, SHA-256.
7. ViruSign — база данных малвари, детектируема антивирусом ClamAV.
8. VirusShare — обновляемый репозиторий для исследователей и реверсеров.

Заключение

Теперь, подготовив домашнюю лабораторию и вооружившись рассмотренными в статье инструментами и образцами малвари, можем приступать к практической реализации — анализу кода вредоносного ПО.

Со следующей статьи мы начнем разбираться в реверсе малвари на реальных примерах. Всем удачи в исследованиях!