

1. Внутреннее устройство Windows. 7-е изд. Авторы: Русинович М., Соломон Д., Ионеску А., Йосифович П.

Год: 2017

Уже есть в сети - ее больше как справочник лучше использовать. Особенно когда до дампов памяти дойдем и там про объекты ядра разговаривать будем.

2. The art of memory forensics

<https://www.memoryanalysis.net/amf>

3. Криминалистика компьютерной памяти на практике. Как эффективно анализировать оперативную память

<https://e.lanbook.com/book/314951?category=1554>

4. Брайан Керри Криминалистический анализ файловых систем

Publisher: Питер | ISBN: 5469013111 | edition 2007

Была вроде посвежее редакция, не вспомню уже от какого года. Оригинал на английском: File System Forensic Analysis, Brian Carrier, 2005

5. Эндрю Пиз: Активное выявление угроз с Elastic Stack. Построение надежного стека безопасности

6. Андрей Мирошников - Мониторинг безопасности Windows, 2018

Вдруг кому еще будет интересно - **список книг по реверсу**

1. Reverse Engineering for Beginners

Можно скачать русскую версию бесплатно прямо с сайта.

<https://beginners.re/>

2. The IDAPRO BOOK. Хорошая книжка про знаменитый дизассемблер иду. При желании, и книгу и саму, довольно свежую выложенную иду, можно найти в сети.

<https://www.amazon.com/IDA-Pro-Book-Unofficial-Disassembler/dp/1593272898>

3. Practical Malware Analysis

https://www.amazon.com/Practical-Malware-Analysis-Hands-Dissecting/dp/1593272901/ref=pd_aw_fbt_img_m_sccl_2/130-7265049-1157222?pd_rd_w=xEDFj&content-id=amzn1.sym.6d90cd56-3eed-4d23-b409-a3b634cfdc4d&pf_rd_p=6d90cd56-3eed-4d23-b409-a3b634cfdc4d&pf_rd_r=DRWF8RE8ZKTP9B5SC EKS&pd_rd_wg=eWawf&pd_rd_r=d0fe0dd2-7c24-42e8-aa6b-cdcef92682c4&pd_rd_i=1593272901&psc=1

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

https://www.amazon.com/dp/1118787315/ref=sspa_mw_detail_0?ie=UTF8&psc=1&sp_csd=d2lkZ2V0TmFtZT1zcF9waG9uZV9kZXRhaWwpl3NParams

5. Руткиты и буткиты

https://www.ozon.ru/product/rutkity-i-butkity-rodionov-evgeniy-matrosov-aleks-504419925/?__rr=1&abt_att=1

Полезная подборка различных дистрибутивов и сопутствующего ПО.

Список полезных дистрибутивов для пентестеров, OSINT специалистов, форензики и других направлений в сфере информационной безопасности:

ISO:

- [Kali Linux](#);
- [BackBox](#);
- [Predator-OS](#);
- [Tails](#);
- [Kodachi](#);
- [Parrot](#);
- [CSI Linux](#);
- [CAINE](#);
- [Tsurugi Linux](#);
- [AthenaOS](#);
- [Forlex](#);
- [Paladine edge](#);
- [Whonix](#);
- [ChallengerOS](#).

ISO standard:

- [Ubuntu](#) - Ver. 22.10;
- [Windows 11](#) - Ver. 22H2;
- [MacOs](#) - Ver. Ventura.

Virtual Machine:

- [OffenOsint](#) — OSINT;
- [Commando-VM](#) — CyberSec;
- [ThreatPursuit-VM](#) — Cyber threat intelligence;
- [Flare-VM](#) — Digital Forensics;
- [Remnux](#) — Analysis Malware - Digital Forensics;
- [SANS/SIFT Workstation](#) — Digital Forensics.

Emulaotri Android:

- [WSA - Windows Subsystem per Android](#);
- [BlueStack](#);

- [NoxPlayer](#);
- [Genymotion](#);
- [Android-Emulators](#).

ПО для виртуализации:

- [VirtualBox](#) - [Документация](#);
- [VMWARE](#) - [Документация](#);
- [Hyper-V](#) - [Документация](#);
- [Kernel Virtual Machine](#) - [Документация](#);
- [UTM Virtualizzatore per MAC](#) - [Документация](#).

ПО для создания live USB:

- [Rufus](#) - [Документация](#);
- [Arsenal Recon](#) - [Документация](#);
- [Ventoy](#) - [Документация](#);
- [Balena Etcher](#) - [Документация](#);
- [Easy2Boot](#) - [Документация](#).

- [Обзор криминалистических артефактов Windows](#)
- [Практические приёмы работы в Wireshark.](#)

Если нужна дополнительная информация и Вы хотите прокачать свои знания работы с **Wireshark**, то я собрал небольшую подборку материала с хабра. Некоторые статьи хоть и старые, но в них очень много актуальной информации, поэтому берите на заметку:

- [Фильтры Wireshark;](#)
- [Wireshark Mindmap;](#)
- [Анализ SSL/TLS трафика в Wireshark;](#)
- [Wireshark для всех. Лайфхаки на каждый день;](#)
- [Как легко расшифровать TLS-трафик от браузера в Wireshark;](#)
- [Фильтры захвата для сетевых анализаторов \(tcpdump, Wireshark, Paketyzer\);](#)
- [Мониторинг трафика на коммутаторах при помощи Wireshark](#)

- Компьютерные сети

• Для тех, кто начал осваивать тему компьютерных сетей, возможно будет интересно: Курс Андрея Сорокина на HE полностью бесплатный

- [Организация сетей TCP/IP;](#)
- [Анализатор сети Wireshark;](#)
- [Прикладной уровень;](#)
- [Протокол HTTP;](#)
- [HTTP в текстовом режиме;](#)
- [Кэширование в HTTP;](#)
- [HTTP в Wireshark](#) [новый выпуск].

➡ Ссылка на плейлист: <https://www.youtube.com/>

