**Учреждение образования**

**«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»**

**Кафедра интеллектуальных информационных технологий**

**Отчет по лабораторной работе №7**

**по курсу «СиМОИБ»**

**на тему: «Исследование операционной системы Windows и отдельных программ с помощью различных утилит»**

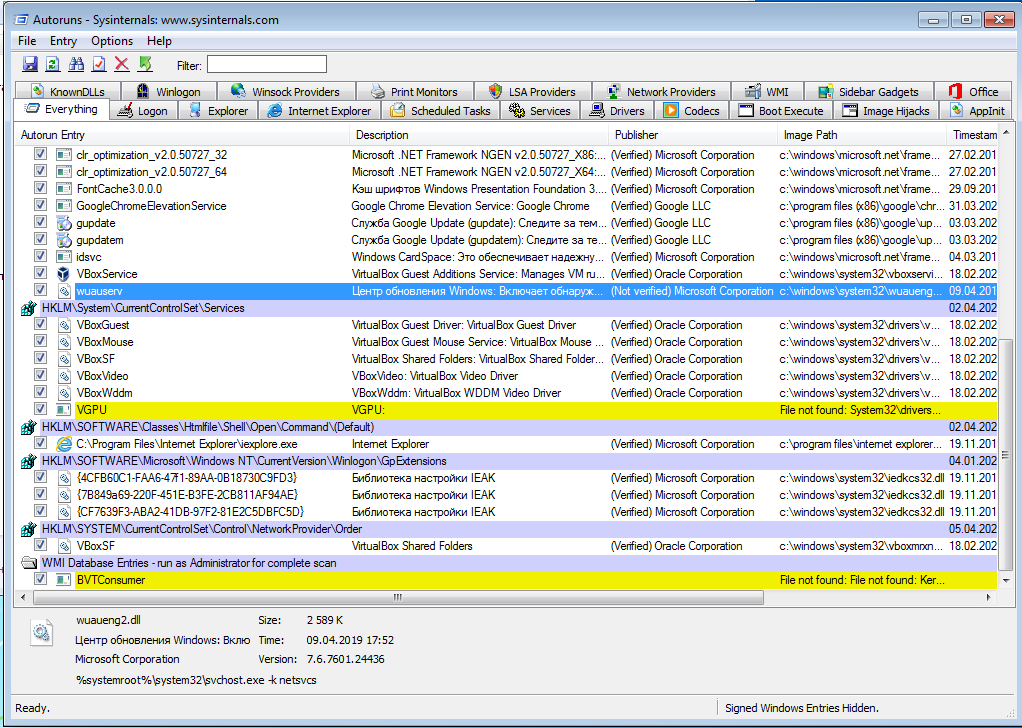
|  |  |
| --- | --- |
| **Выполнил:** | **Студент группы 821703**  **Веренич К.О.** |
| **Проверил:** | **Захаров В. В.** |
|  |  |

МИНСК

2020

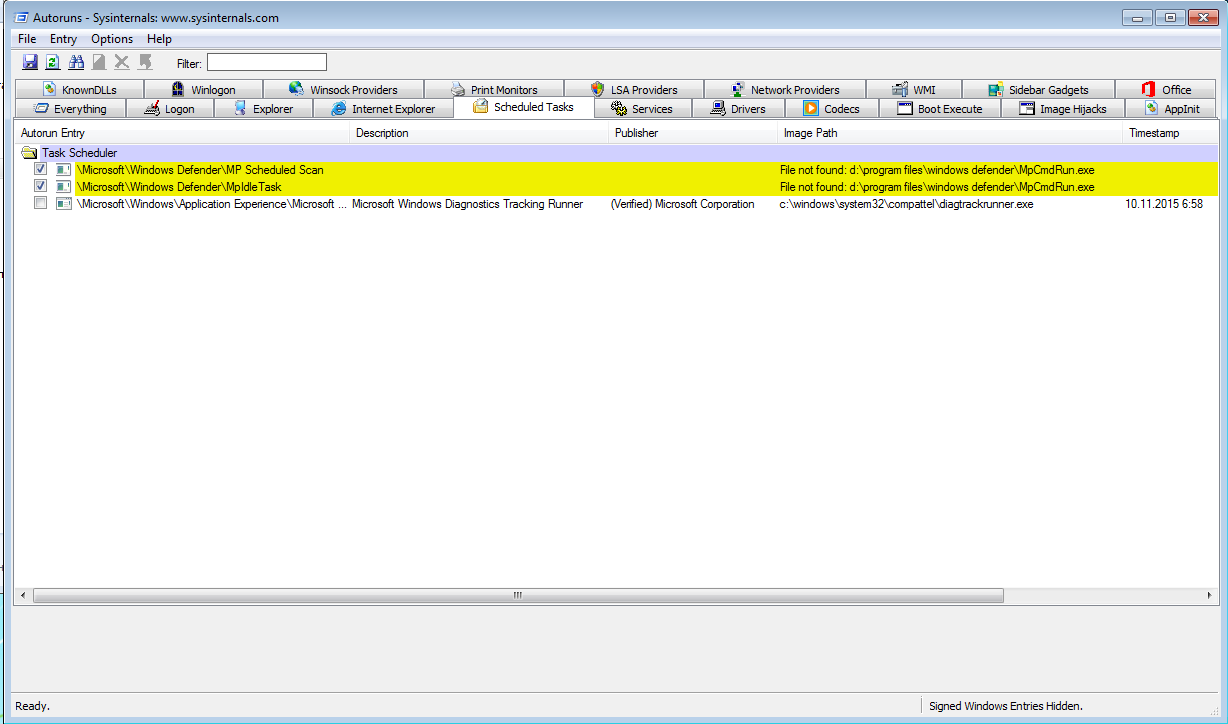
**Задание 1:** На основном компьютере запустить утилиту autoruns. Определить автоматически загружаемые программы и библиотеки. Просмотреть содержимое различных разделов. Выявить некорректные или отсутствующие программы.

1. Открытие программы Autoruns

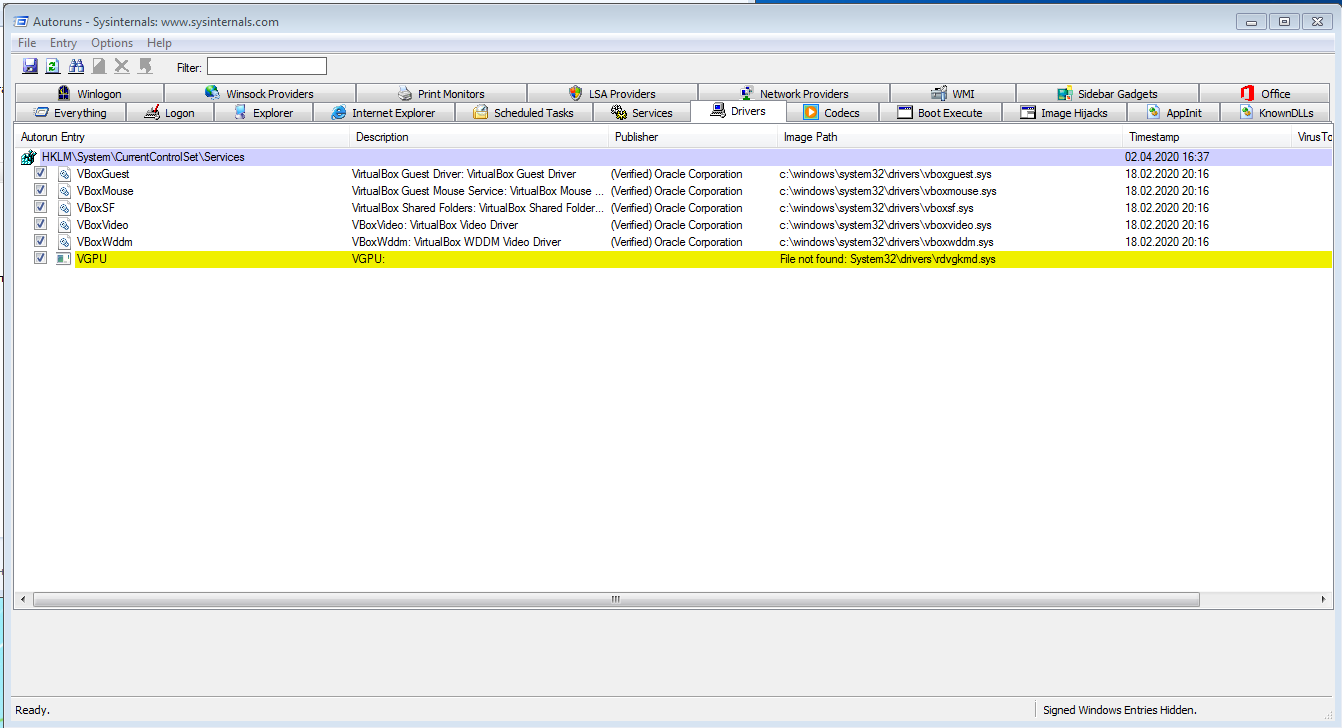


В программе по умолчанию открыт раздел Everything (Все) в котором собраны все автоматически загружаемые программы, библиотеки, службы и т.д.

Другие разделы классифицируют автоматически исполняющиеся объекты находящиеся в разделе Everything (Все). Например среди разделов можно найти задания планировщика задач Windows.



Или автоматически загружаемые драйвера устройств

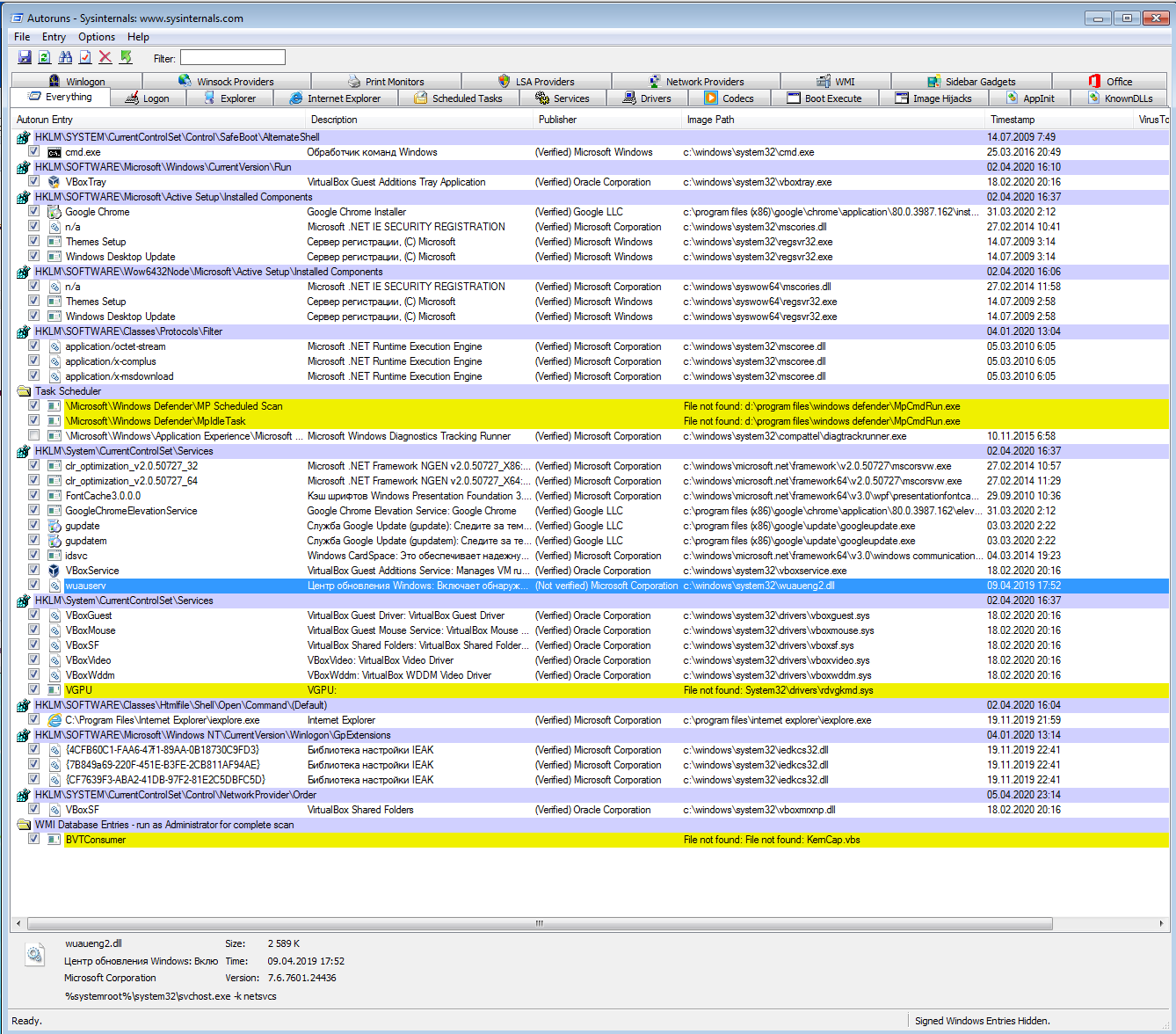


Как можно заметить некоторые пункты в списках выделены цветом, это означает что с этим объектом что-то не так, например пояснение к объекту выделенному желтым цветом содержится в колонке Image Path (Путь к образу) - File not found (Файл не найден), а выделение красным цветом означает что объект автозагрузки не имеет цифровой подписи.

1. Произведем очистку от некорректных или отсутствующих объектов автозагрузки.

Удобнее всего производить очистку на вкладке Everything (Все), так как сразу можно видеть все некорректно работающие программы.

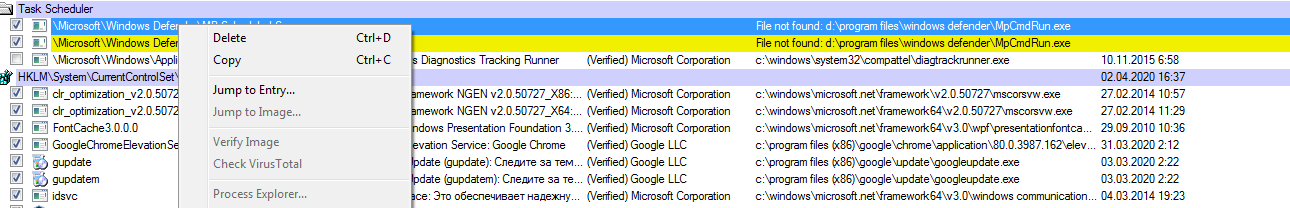
Ниже представлена вкладка Everything (Все) для используемой машины.



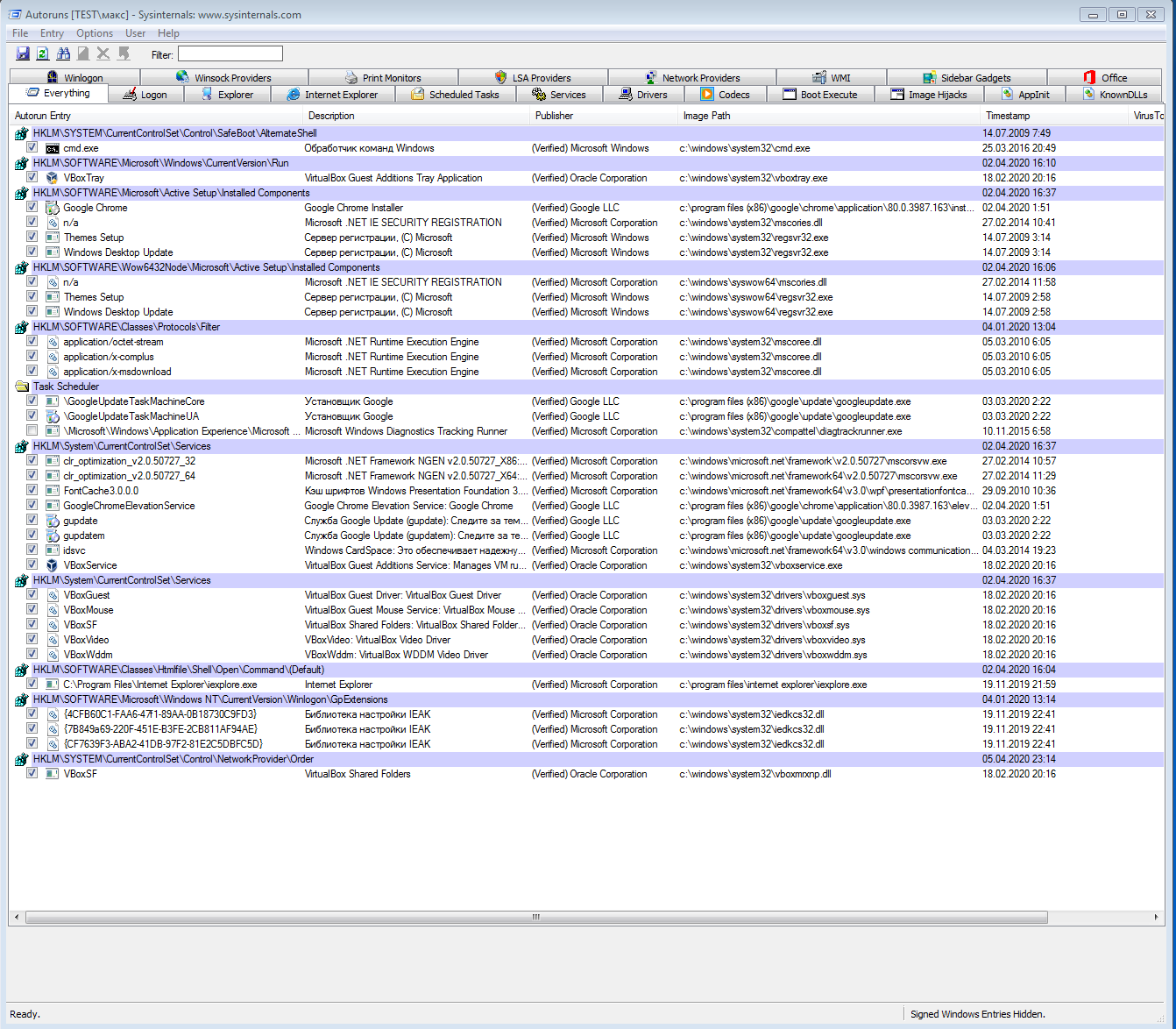
В ней можно наблюдать три пункта выделенных желтым цветом, из них:

* два задания планировщика заданий
* одна служба

У всех ошибка: File not found (Файл не найден), удалим эти пункты из элементов автозагрузки

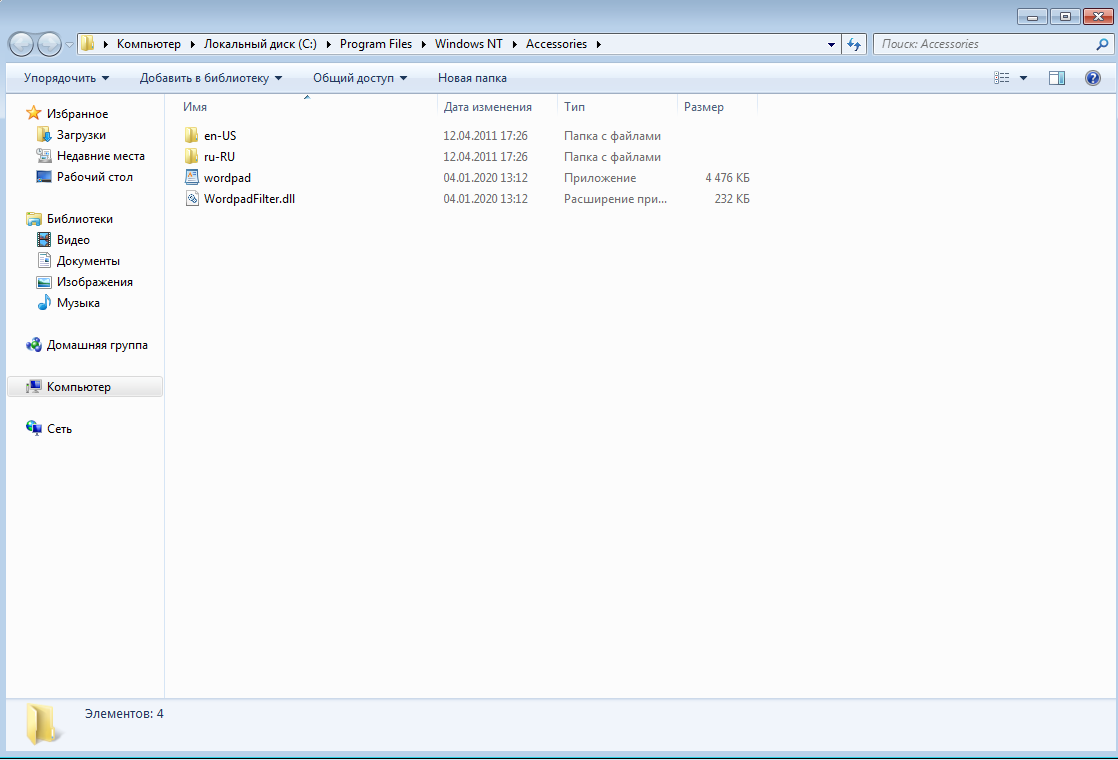


Вот как выглядит раздел Everything (Все) после удаления некорректно функционирующих элементов автозагрузки

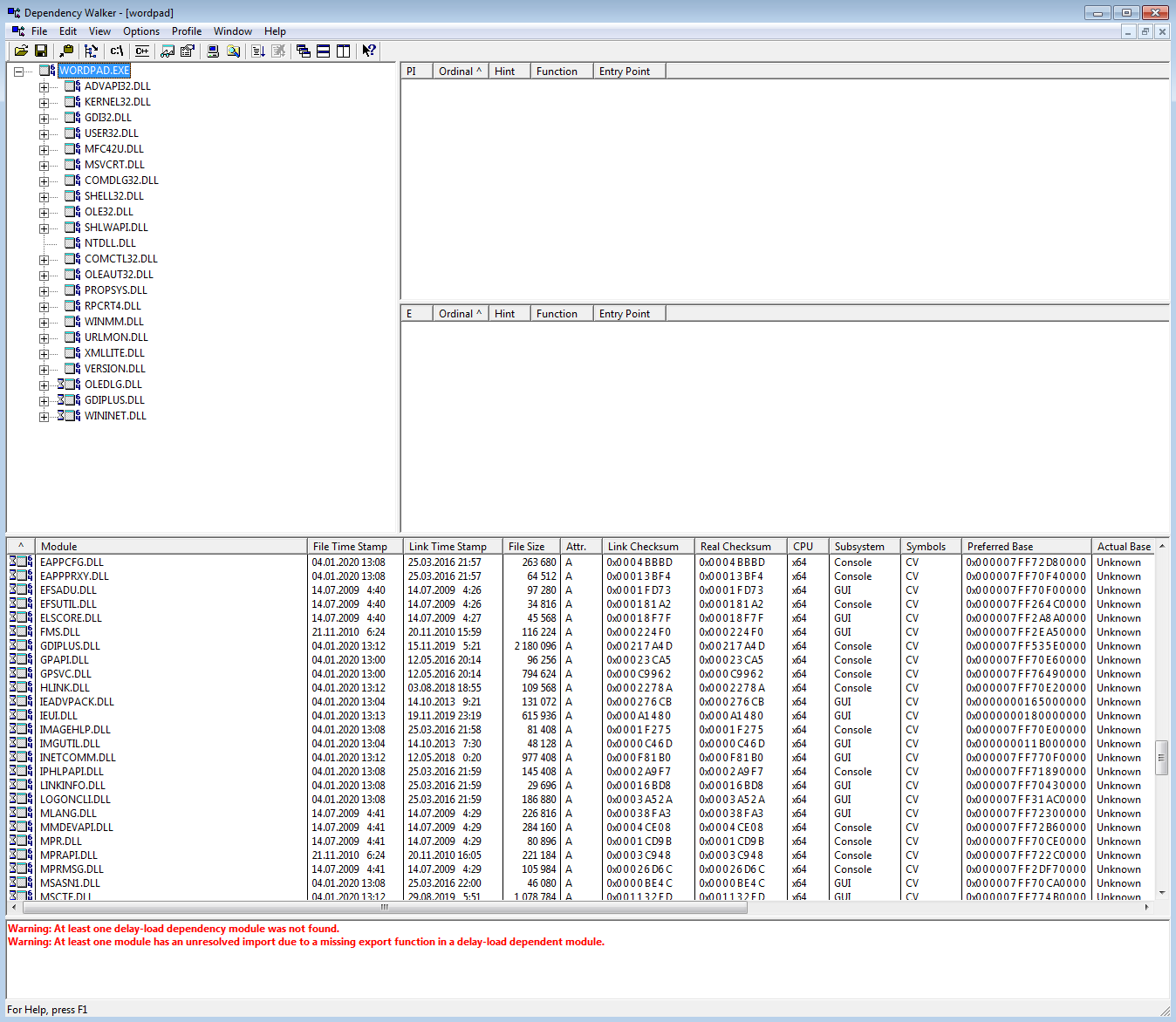
****

**Задание 2:** Выбрать какое-либо приложение (Wordpad, Notepad и т.д.). С помощью утилиты Dependency Walker определить с какими модулями связано данное приложение. С помощью Process Explorer определить список модулей загруженных в контексте приложения. Получить информацию о каждом загруженном модуле (производитель, место расположения и т.д.), сделать вывод о том, можно ли доверять этому модулю.

Для теста выбрана стандартная программа Windows - Wordpad

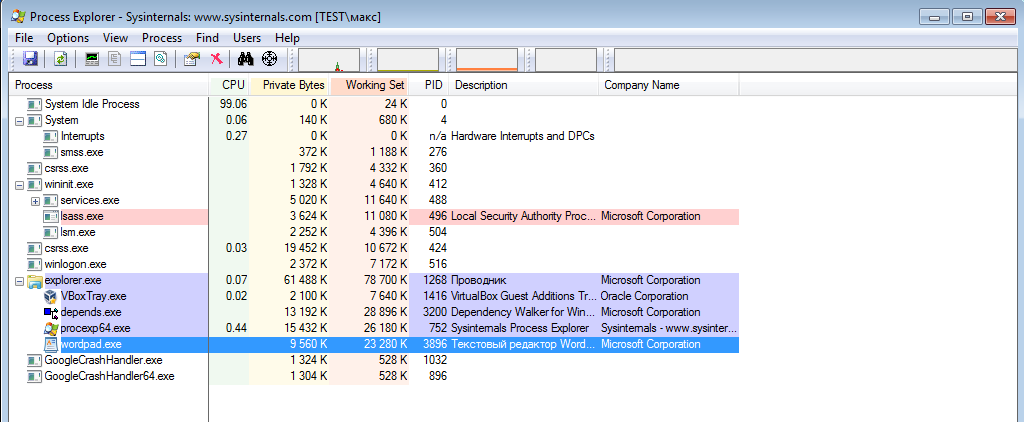


Откроем исполняемый (.exe) файл в программе Dependency Walker

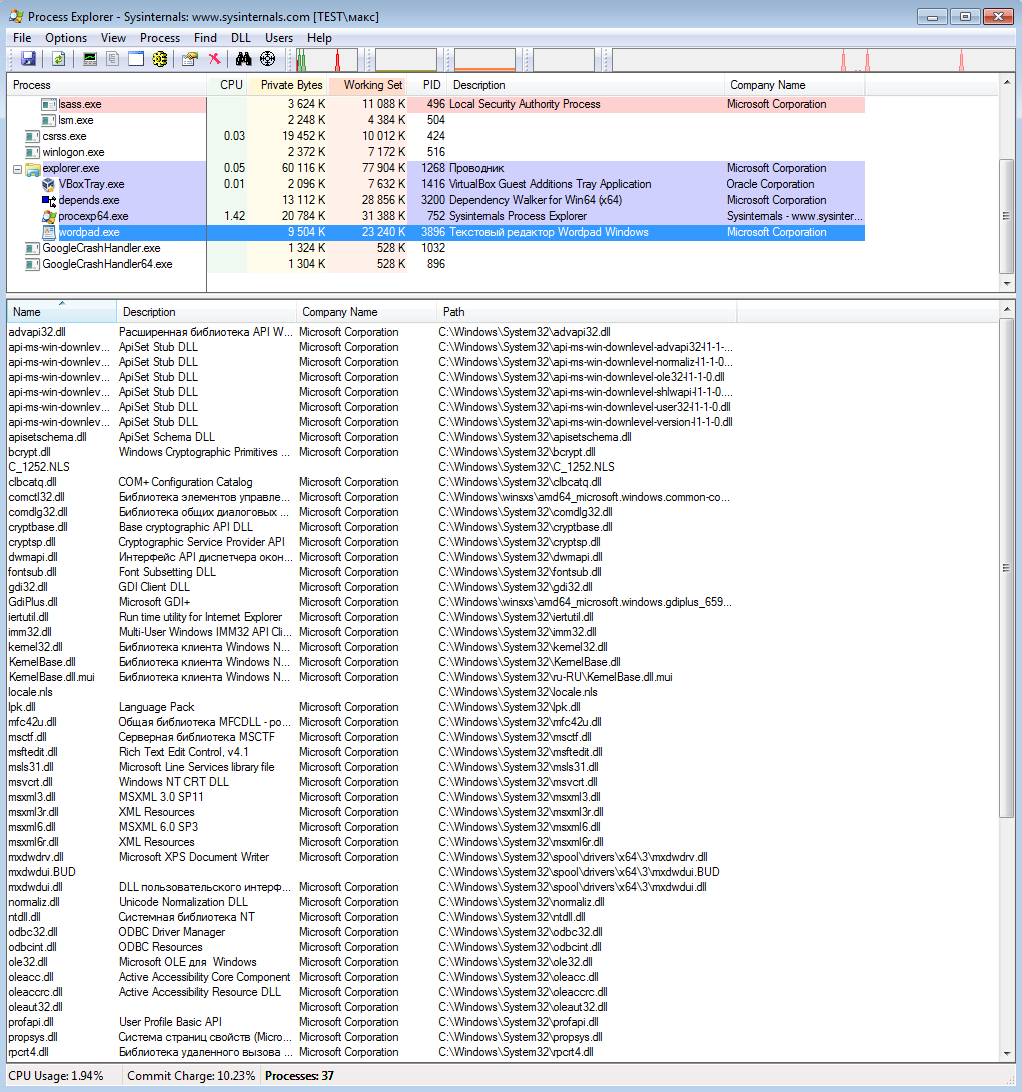


Слева вверху мы можем наблюдать список зависимостей программы Wordpad.

Откроем программу Process Explorer и запустим Wordpad.

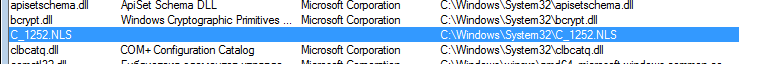


В меню выберем пункт View DLLs (Просмотреть DLL)

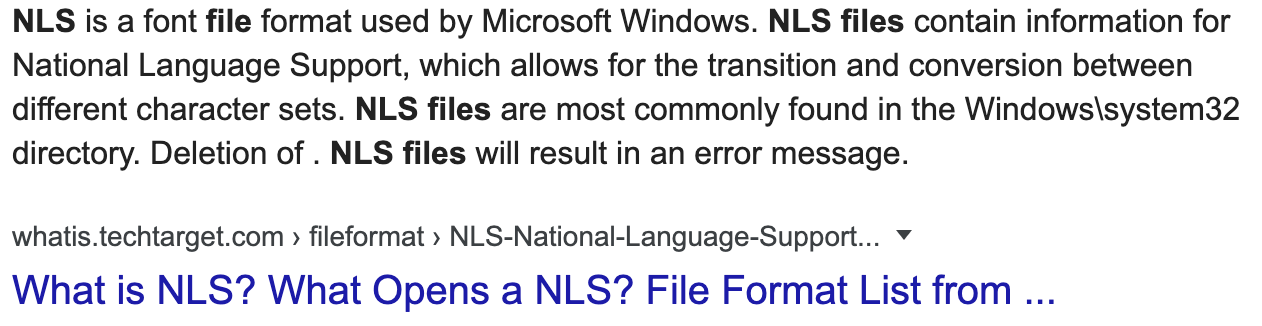


Все модули (.dll) имеют в качестве разработчика Microsoft Corporation, компанию создающую систему Windows, соответственно такие файлы являются полностью безопасны и им можно доверять.

Обратим внимание на несколько компонентов у которых разработчик не указан, например C\_1252.NLS

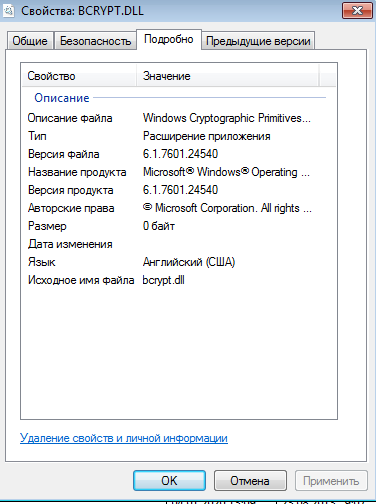
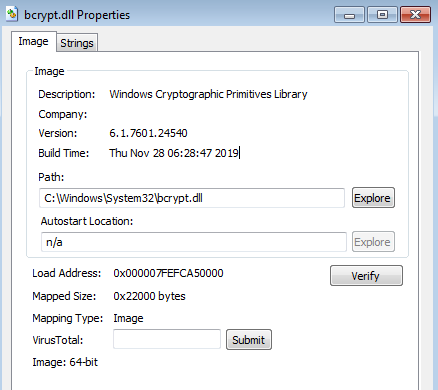


Поискав информацию про данный файл в интернете, можно узнать что это файл кодировки С1252, и он полностью безопасен, так как тоже создан компанией Microsoft.



Также проанализируем один файл с указанным разработчиком например bcrypt.dll

Process Explorer Dependency Walker

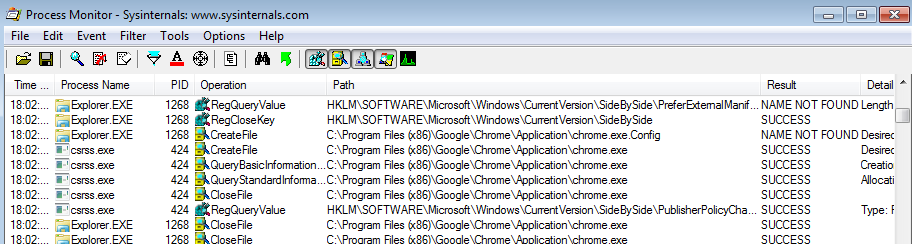


Вся информация о модуле совпадает, можно найти версию файла, разработчика и описание, соответственно данный файл полностью безопасен.

**Задание 3.** С помощью утилит Regmon, Filemon или Process Monitor выполнить мониторинг обращений выбранного приложения к реестру и файловой системы.

Будем использовать программу ProcessMonitor.

Включим параметры Show registry activity (Показать активность в реестре) и Show file system activity (Показать активность в файловой системе)



С помощью поиска найдем все с чем связана программа Wordpad



Как мы здесь видим, в 18.02 происходил вызов системной функции CreateFile а за ней ReadFile. Данные функции являются обращениями программы к файловой системе Windows.

**Вывод**

В ходе выполнения данной лабораторной работы были изучены различные утилиты для мониторинга состояния операционной системы Windows, с помощью которых можно найти обращения программы к реестру и файловой системе, список модулей загруженных в контексте программы, а также элементы автозагрузки системы.

Autoruns - программа позволяющая просмотреть все элементы автозапуска системы вплоть до драйверов и планировщика заданий, в основном она используется для выявления и устранения нежелательных элементов автозагрузки. Стоит заметить что программа предоставляет достаточно широкую функциональность, действия в этой программе (например в разделе с драйверами или службами) при неправильном использовании могут нанести вред компьютеру.

Утилита Process Monitor позволяет получать подробную информацию о взаимодействии процессов, использовании аппаратных ресурсов, сетевой активности, операциях взаимодействия с файловой системой, взаимодействии программы с реестром, а также о вызове программой системных функций.

Dependency Walker - программа для выявления зависимостей исполняемых файлов и представления этих зависимостей в иерархическом виде.