**ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №7**

**Тема: «Утилиты Windows»**

**Цель работы:** практическое изучение возможностей утилит Windows на примере наиболее характерных операций.

***Задание №1:*** Запустите утилиту Process Explorer и выполните задания.

***Ход выполнения***

При запуске утилиты загруженность процессора составила около 40%, загруженность ОЗУ 15% (800 Мб., 900Мб.).

Чтобы свернуть окно необходимо нажать ПКМ по процессу и в подменю Window выбрать Minimize (рис. 1).

Для сочетания клавиш Ctrl+Alt+Delete назначен запуск Process Explorer (рис. 2).

Процесс explorer.exe имеет 42 потока (рис. 3), procexp64.exe имеет 8 потоков (рис. 4).

Process Explorer запускается из папки с загрузками (рис. 5), и использует 2-3% ресурсов CPU и 20 Мб. ОЗУ (рис. 6).

Изменён порядок столбцов программы (рис. 7).

Количество процессов, запущенных в системе: 45 (рис. 8).

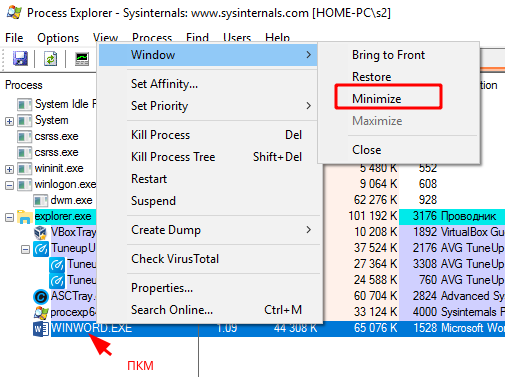
Отсортировать процессы по какому-либо параметру можно, нажав на столбец этого параметра. Процессом, занимающим большее количество ОЗУ является explorer.exe (PID 3176) (рис. 9).

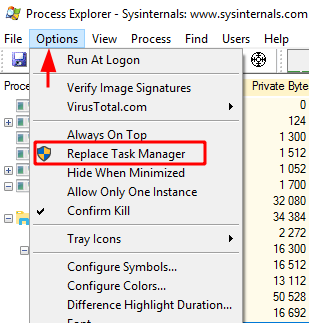
Дерево процессов представлено на рисунке 10. В нём имеется 10 процессов-родителей и 3 процесса, не имеющих родителей.

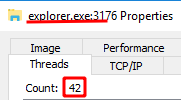
Применив сортировку по столбцу CPU было определено, что System Idle Process использует больше всего процессорных ресурсов (рис. 11).

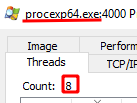
При удалении процесса explorer «сиротами» остались процессы VboxTray.exe и procexp64.exe (рис. 12).

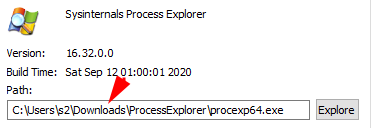
System Idle Process — Процесс простоя системы, который показывает процент времени, в течение которого процессор простаивает. Memory Compression — Функция сжатия оперативной памяти в Windows 10 предназначена для ускорения работы (отзывчивости) системы за счет хранения части страниц в оперативной памяти в сжатом виде.

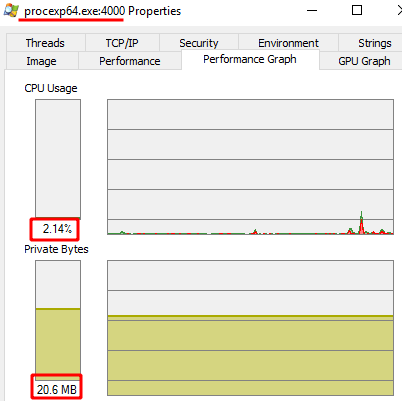
 Рисунок 1 — Сворачивание окна

Рисунок 2 — Назначение запуска на сочетание клавиш

Рисунок 3 — Количество потоков у проводника

Рисунок 4 — Количество потоков у Process Explorer

Рисунок 5 — Папка запуска Process Explorer

Рисунок 6 — Использование ресурсов программой

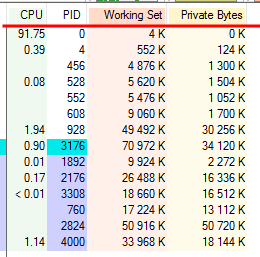
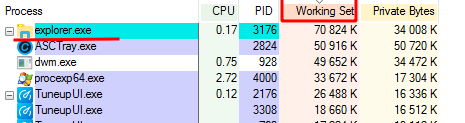
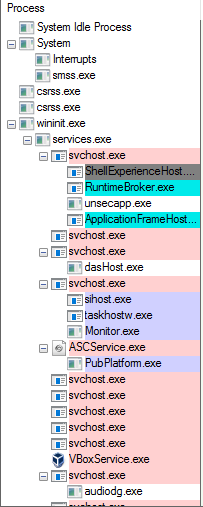
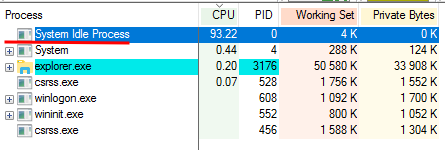
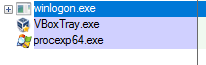
Рисунок 7 — Столбцы программы

Рисунок 8 — Количество процессов, запущенных в системе

Рисунок 9 — Сортировка процессов

Рисунок 10 — Дерево процессов

Рисунок 11 — Самый прожорливый процесс

Рисунок 12 — Процессы, оставшиеся после завершения explorer

***Задание №2:*** Запустите утилиту Process Monitor и выполните задания.

***Ход выполнения***

Для отображения запросов интересующего процесса необходимо создать подобный фильтр (рис. 13). Для отображения только вызовов, связанных с реестром, необходимо выбрать соответствующий фильтр (рис. 14). Последнее обращение было к ключу «HKCR\CLSID\{56AD4C5D-B908-4F85-8FF1-7940C29B3BCF}\Instance» (рис. 15). Тип обращения «RegOpenKey» (рис. 15). Перейдя в реестр, к нужному файлу, он не был найден (рис. 16), что и было в результате выполнения запроса диспетчером задач (NAME NOT FOUND) (рис. 15).

Вызовы были отфильтрованы по активности файловой системы (рис. 17). Последнее обращение было к файлу «C:\Windows\System32\OneCoreCommonProxyStub.dll». Тип обращения: «ReadFile». Открытый файл в проводнике (рис. 18).

Фильтр, исключающий процессы от Microsoft Corporation (рис. 19).

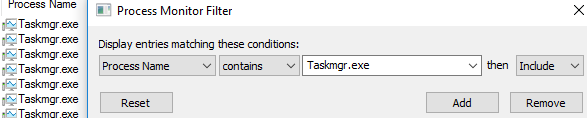
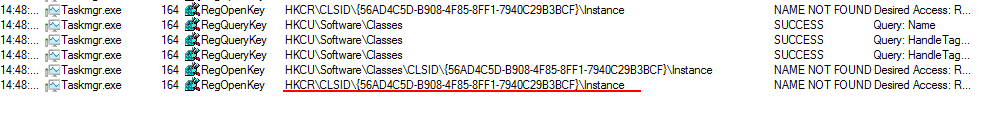
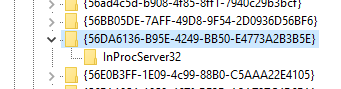
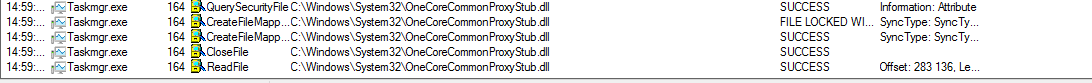
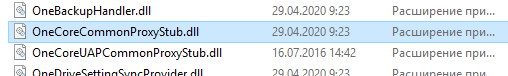
Рисунок 13 — Фильтрация по имени процесса

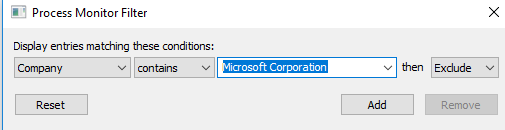
Рисунок 14 — Фильтрация вызовов к реестру

Рисунок 15 — Последнее обращение к реестру

Рисунок 16 -Расположение в реестре

Рисунок 17 — Активность файловой системы

Рисунок 18 — Открытый файл

Рисунок 19 — Фильтр

***Задание №3:*** Запустите утилиту ZoomIt и выполните задания.

***Ход выполнения***

Посредством ZoomIt увеличена зона системного трея и обведён значок ZoomIt (рис. 20).

Таймер на 1 минуту над затемнённым рабочим столом (рис. 21).

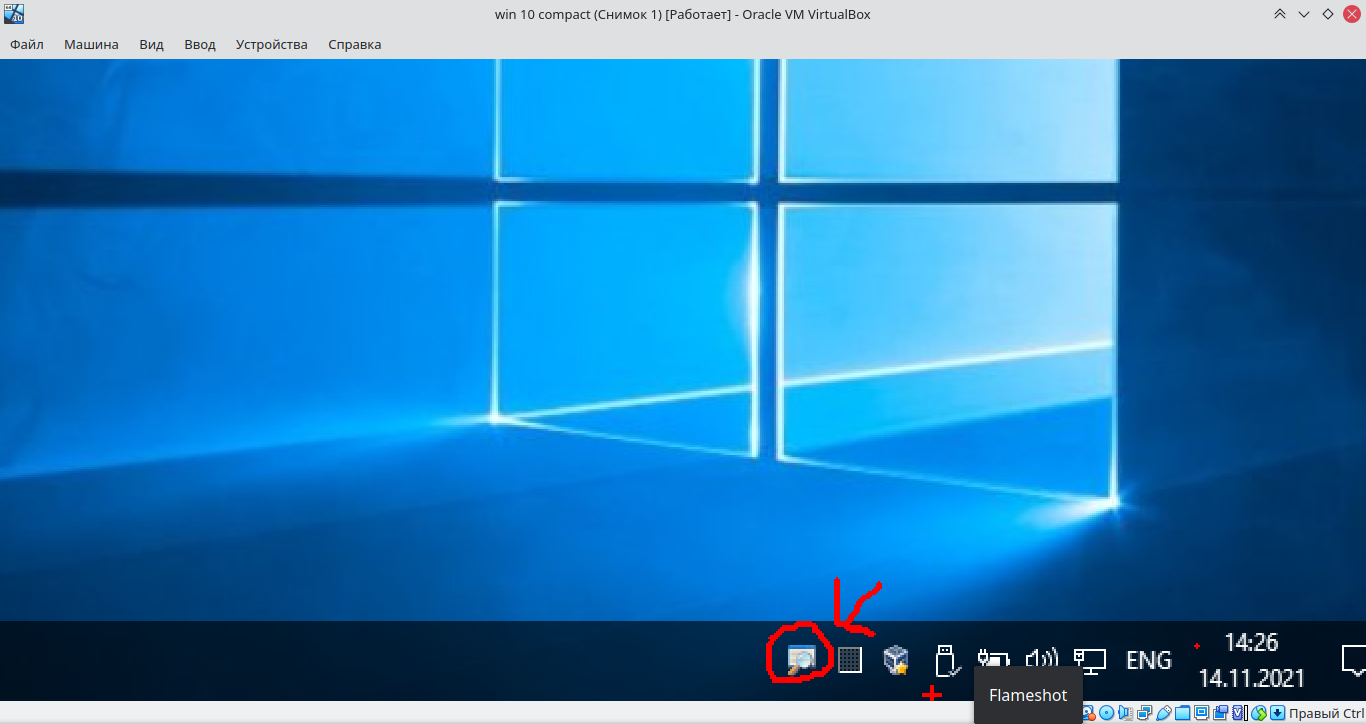
Рисунок 20 — Увеличение зоны системного трея

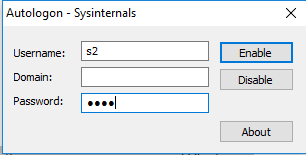
Рисунок 21 - Таймер

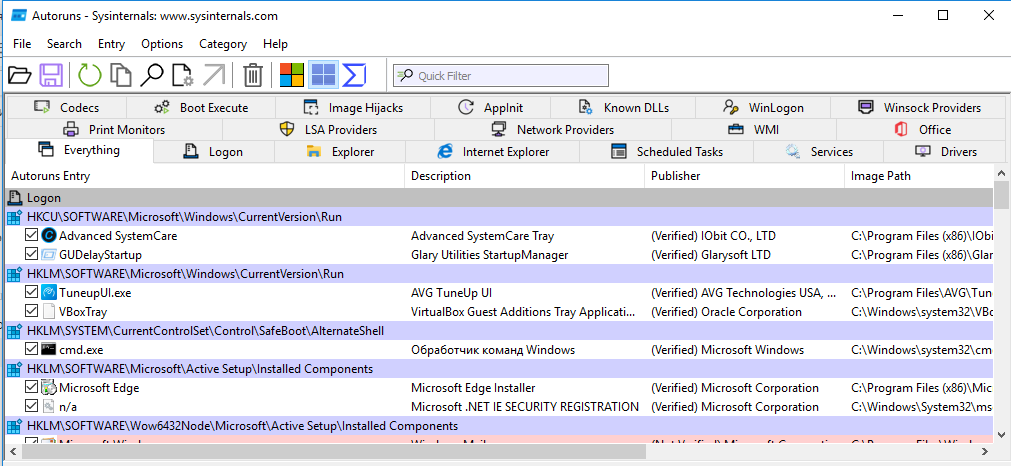
***Задание №4:*** Выберите две любые утилиты Sysinternals, скачайте их и опишите.

***Ход выполнения***

Autologon (рис. 22) позволяет легко настроить встроенный механизм автовхода Windows. Вместо того, чтобы ждать, пока пользователь введет свое имя и пароль, Windows использует учетные данные, вводимые с помощью autologon, которые шифруются в реестре, для автоматического входа в систему указанного пользователя.

Autoruns. Эта утилита, которая обладает наиболее полными знаниями о местах автозапуска любого монитора запуска, показывает вам, какие программы настроены для запуска во время загрузки системы или входа в систему, а также при запуске различных встроенных приложений Windows, таких как Internet Explorer, Explorer и медиаплееры. К таким программам и драйверам относятся программы и драйверы в папке автозагрузки, Run, RunOnce и других разделах реестра. Autoruns сообщает о расширениях оболочки проводника, панелях инструментов, вспомогательных объектах браузера, уведомлениях Winlogon, службах автозапуска и многом другом. Autoruns выходит далеко за рамки других утилит автозапуска.

Рисунок 22 — Autologon

Рисунок 23 — Autoruns