МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)

Институт №8 «Компьютерные науки и прикладная математика»
Кафедра 806 «Вычислительная математика и программирование»

Лабораторная работа №3
по курсу «Операционные системы»

Выполнил: К. С. Шульц
Группа: М8О-208БВ-24
Преподаватель: Е. С. Миронов

Москва, 2025

Условие:

Родительский процесс создает два дочерних процесса. Взаимодействие между процессами организовано через отображаемые файлы (memory-mapped files). Родительский и дочерние процессы должны быть представлены разными программами. Родительский процесс принимает от пользователя строки произвольной длины и записывает их в область разделяемой памяти MMF1. Процессы child1 и child2 производят работу над строками, передавая данные последовательно через MMF2. Child2 записывает результат своей работы в область разделяемой памяти MMF3, откуда родительский процесс читает результат.

Цель работы:

Освоение принципов работы с файловыми системами, обеспечение обмена данных между процессами посредством технологии «File mapping»

Задание:

Обработка строк: Child1 переводит строки в нижний регистр. Child2 убирает все задвоенные пробелы.

Вариант: 14

Описание программы

Метод решения

Данная программа реализует многопроцессную обработку текстовых данных с использованием отображаемых файлов (memory-mapped files) для межпроцессного взаимодействия. Родительский процесс читает строки из стандартного ввода и направляет их через цепочку дочерних процессов, каждый из которых выполняет преобразование данных. Взаимодействие организовано через разделяемую память, что обеспечивает высокую производительность при обмене данными.

Основные компоненты:

Parent - управляет созданием областей разделяемой памяти, запуском дочерних процессов, принимает пользовательский ввод и выводит конечный результат;

Child1 - приводит текст к нижнему регистру;

Child2 - удаляет все задвоенные пробелы;

Разделение системных вызовов в отдельную библиотеку systemCall.

Описание программы

Структура проекта:

lab3/

    include/

        systemCall.h // Заголовочный файл библиотеки

    src/

        systemCall.cpp // Реализация системных функций

        parent.cpp // Родительский процесс

        child1.cpp // Дочерний процесс 1 (нижний регистр)

        child2.cpp // Дочерний процесс 2 (удаление пробелов)

    CMakeLists.txt

Основные типы данных:

1.Структура mmfT (memory-mapped file)

Содержит дескриптор области памяти, указатель на данные и размер области

На Windows использует HANDLE, на Linux - файловые дескрипторы

Позволяет организовать разделяемый доступ к памяти между процессами

2.Структура process (информация о процессе)

Хранит идентификатор запущенного процесса

На Windows содержит подробную информацию о процессе, на Linux - просто номер процесса (PID)

Содержит флаг is-valid, который показывает, работает ли процесс корректно

3.Строки std::string

4.Логические флаги (bool)

Принцип работы с типами данных:

Программа создает несколько областей разделяемой памяти mmfT, через которые передаются строки std::string. Каждый дочерний процесс управляется через свою структуру process, а логические флаги следят за тем, чтобы вся система работала без ошибок. Данные передаются через общую память, что исключает необходимость сериализации и копирования.

Основные функции программы:

MMFCreate() - создает новую область разделяемой памяти

MMFOpen() - открывает существующую область разделяемой памяти

MMFClose() - закрывает область памяти, освобождая ресурсы

WriteToMMF() - записывает строку в разделяемую память

ReadFromMMF() - читает строку из разделяемой памяти

ClearMMF() - очищает область памяти

ProcessCreateWithMMF() - запускает дочерний процесс с передачей имен MMF

ProcessTerminate() - принудительно завершает процесс

Используемые системные вызовы:

Для Windows:

CreateFileMappingA() - создание объекта проекции файла;

MapViewOfFile() - отображение файла в память;

OpenFileMappingA() - открытие существующего объекта проекции;

UnmapViewOfFile() - отмена отображения памяти;

CreateProcessA() - создание процесса;

CloseHandle() - закрытие дескриптора;

TerminateProcess() - принудительное завершение;

Для Linux:

shm open() - создание/открытие разделяемой памяти;

mmap() - отображение памяти в адресное пространство;

munmap() - отмена отображения памяти;

ftruncate() - установка размера разделяемой памяти;

fork() - создание процесса;

exec() - загрузка новой программы;

close() - закрытие дескриптора;

kill() - отправка сигнала процессу;

Результаты

Разработана многопроцессная система для конвейерной обработки текстовых данных, состоящая из трех взаимосвязанных процессов, взаимодействующих через систему отображаемых файлов (memory-mapped files).

Ключевые результаты:

- Реализованы три области разделяемой памяти, образующие последовательный конвейер обработки;

- Обеспечена надежная передача текстовых данных от родительского процесса через два дочерних процесса с использованием общей памяти;

- Реализована обработка системных ошибок, дочерние процессы корректно завершаются при получении сигнала завершения от родительского процесса;

- Высокая производительность при обработке данных за счет использования механизма разделяемой памяти вместо традиционных каналов;

- Обеспечена кроссплатформенность - программа корректно работает как в Windows, так и в Linux системах.

Выводы

В ходе лабораторной работы была создана программа для обработки текста, которая использует три процесса, взаимодействующих через общую память (memory-mapped files).

Что получилось:

- Научились работать с общей памятью для обмена данными между процессами
- Сделали программу, которая работает одинаково хорошо в Windows и Linux
- Данные передаются быстро, так как не нужно их копировать несколько раз
- Программа надежно работает и правильно закрывает все ресурсы
- Общая память оказалась удобнее и быстрее обычных каналов

Исходная программа

systemCall.cpp

```cpp
#include <iostream>

#include "systemCall.h"

#ifdef _WIN32
#include <tchar.h>
#endif

bool MMFCreate(mmfT* mmf, const char* name, size_t size) {
    if (!mmf) {
        std::cerr << "Error: Null pointer in MMFCreate" << std::endl;
        return false;
    }

#ifdef _WIN32
    mmf->handle = CreateFileMappingA(
        INVALID_HANDLE_VALUE,
        NULL,
        PAGE_READWRITE,
        0,
        size,
        name
    );

    if (mmf->handle == NULL) {
        std::cerr << "Error: CreateFileMapping failed for " << name << std::endl;
        return false;
    }

    mmf->data = MapViewOfFile(
        mmf->handle,
        FILE_MAP_ALL_ACCESS,
        0, 0,
        size
    );

#else
    mmf->handle = shm_open(name, O_CREAT | O_RDWR, 0666);
    if (mmf->handle == -1) {
        std::cerr << "Error: shm_open failed for " << name << std::endl;
        return false;
    }

    if (ftruncate(mmf->handle, size) == -1) {
        std::cerr << "Error: ftruncate failed for " << name << std::endl;
        close(mmf->handle);
        return false;
    }

    mmf->data = mmap(
        NULL,
        size,
        PROT_READ | PROT_WRITE,
        MAP_SHARED,
        mmf->handle,
        0
    );

    if (mmf->data == MAP_FAILED) {
        std::cerr << "Error: mmap failed for " << name << std::endl;
        close(mmf->handle);
        return false;
    }
#endif

    if (!mmf->data) {
        std::cerr << "Error: Memory mapping failed for " << name << std::endl;
#ifdef _WIN32
        CloseHandle(mmf->handle);
#else
        close(mmf->handle);
#endif
        return false;
    }

    mmf->size = size;
    memset(mmf->data, 0, size);
    std::cout << "Created MMF: " << name << " size: " << size << std::endl;
    return true;
}

bool MMFOpen(mmfT* mmf, const char* name, size_t size) {
    if (!mmf) {
        std::cerr << "Error: Null pointer in MMFOpen" << std::endl;
        return false;
    }
#ifdef _WIN32
    mmf->handle = OpenFileMappingA(
        FILE_MAP_ALL_ACCESS,
        FALSE,
        name
    );

    if (mmf->handle == NULL) {
        std::cerr << "Error: OpenFileMapping failed for " << name << std::endl;
        return false;
    }

    mmf->data = MapViewOfFile(
        mmf->handle,
        FILE_MAP_ALL_ACCESS,
        0, 0,
        size
    );
#else
    mmf->handle = shm_open(name, O_RDWR, 0666);
    if (mmf->handle == -1) {
        std::cerr << "Error: shm_open failed for " << name << std::endl;
        return false;
    }

    mmf->data = mmap(
        NULL,
        size,
        PROT_READ | PROT_WRITE,
        MAP_SHARED,
        mmf->handle,
        0
    );

    if (mmf->data == MAP_FAILED) {
        std::cerr << "Error: mmap failed for " << name << std::endl;
        close(mmf->handle);
        return false;
    }
#endif

    if (!mmf->data) {
        std::cerr << "Error: Memory mapping failed for " << name << std::endl;
#ifdef _WIN32
        CloseHandle(mmf->handle);
#else
        close(mmf->handle);
#endif
        return false;
    }

    mmf->size = size;
    std::cout << "Opened MMF: " << name << std::endl;
    return true;
}

void MMFClose(mmfT* mmf) {
    if (!mmf || !mmf->data) {
        return;
    }

#ifdef _WIN32
    UnmapViewOfFile(mmf->data);
    if (mmf->handle != INVALID_MMF_HANDLE) {
        CloseHandle(mmf->handle);
    }
#else
    munmap(mmf->data, mmf->size);
    if (mmf->handle != INVALID_MMF_HANDLE) {
        close(mmf->handle);
    }
#endif

    mmf->data = nullptr;
    mmf->handle = INVALID_MMF_HANDLE;
    mmf->size = 0;

    std::cout << "Closed MMF" << std::endl;
}

bool WriteToMMF(mmfT& mmf, const std::string& data) {
    if (!mmf.data || data.length() >= mmf.size) {
        return false;
    }
    strcpy(static_cast<char*>(mmf.data), data.c_str());
```

```cpp
    return true;
}

std::string ReadFromMMF(mmfT& mmf) {
    if (!mmf.data) {
        return "";
    }
    return std::string(static_cast<char*>(mmf.data));
}

void ClearMMF(mmfT& mmf) {
    if (mmf.data) {
        memset(mmf.data, 0, mmf.size);
    }
}

process ProcessCreateWithMMF(const char* program, const char* inputName, const char* outputName) {
    process process_info;
    process_info.is_valid = false;

#ifdef _WIN32
    std::string cmd = program;
    cmd += " ";
    cmd += inputName;
    cmd += " ";
    cmd += outputName;

    STARTUPINFOA si;
    ZeroMemory(&si, sizeof(si));
    si.cb = sizeof(si);

    PROCESS_INFORMATION pi;
    ZeroMemory(&pi, sizeof(pi));

    if (CreateProcessA(NULL, (LPSTR)cmd.c_str(), NULL, NULL, TRUE, 0, NULL, NULL, &si, &pi)) {
        process_info.process_info = pi;
        process_info.is_valid = true;
        CloseHandle(pi.hThread);
        std::cout << "Created process: " << program << std::endl;
    } else {
        std::cerr << "Error: CreateProcess failed for " << program << std::endl;
    }
#else
    pid_t pid = fork();
    if (pid == 0) {
        execl(program, program, inputName, outputName, NULL);
        std::cerr << "Error: execl failed for " << program << std::endl;
        exit(1);
    } else if (pid > 0) {
        process_info.pid = pid;
        process_info.is_valid = true;
        std::cout << "Created process: " << program << " PID: " << pid << std::endl;
    } else {
        std::cerr << "Error: fork failed for " << program << std::endl;
    }
#endif
```

```

    return process_info;
}

int ProcessTerminate(process* process_info) {
    if (!process_info || !process_info->is_valid) {
        return 0;
    }

#ifdef _WIN32
    TerminateProcess(process_info->process_info.hProcess, 0);
    WaitForSingleObject(process_info->process_info.hProcess, 1000);
    CloseHandle(process_info->process_info.hProcess);
#else
    kill(process_info->pid, SIGTERM);
    waitpid(process_info->pid, NULL, 0);
#endif

    process_info->is_valid = false;
    std::cout << "Process terminated" << std::endl;
    return 1;
}
```

systemCall.h

```
#ifndef SYSTEMCALL_H
#define SYSTEMCALL_H

#include <string>

#ifdef _WIN32
    #include <windows.h>
    #define MMF_HANDLE HANDLE
    #define INVALID_MMF_HANDLE NULL
#else
    #include <unistd.h>
    #include <sys/wait.h>
    #include <sys/mman.h>
    #include <fcntl.h>
    #include <sys/stat.h>
    #define MMF_HANDLE int
    #define INVALID_MMF_HANDLE -1
#endif

typedef struct {
    MMF_HANDLE handle;
    void* data;
    size_t size;
} mmfT;

typedef struct {
#ifdef _WIN32
    PROCESS_INFORMATION process_info;
#else
    pid_t pid;
#endif
    bool is_valid;
} process;

```

```
bool MMFCreate(mmfT* mmf, const char* name, size_t size);
bool MMFOpen(mmfT* mmf, const char* name, size_t size);
void MMFClose(mmfT* mmf);
bool WriteToMMF(mmfT& mmf, const std::string& data);
std::string ReadFromMMF(mmfT& mmf);
void ClearMMF(mmfT& mmf);

process ProcessCreateWithMMF(const char* program, const char* inputName, const char*
    outputName);
int ProcessTerminate(process* process_info);
#endif
```

parent.cpp

```
#include <iostream>
#include <string>

#include "systemCall.h"

int main() {
    mmfT mmf1, mmf2, mmf3;
    process child1, child2;

    mmf1.handle = INVALID_MMF_HANDLE; mmf1.data = nullptr;
    mmf2.handle = INVALID_MMF_HANDLE; mmf2.data = nullptr;
    mmf3.handle = INVALID_MMF_HANDLE; mmf3.data = nullptr;

    std::cout << "Creating MMF and processes..." << std::endl;

    const size_t MMF_SIZE = 1024;
    if (!MMFCreate(&mmf1, "parent_to_child1", MMF_SIZE) ||
        !MMFCreate(&mmf2, "child1_to_child2", MMF_SIZE) ||
        !MMFCreate(&mmf3, "child2_to_parent", MMF_SIZE)) {
        std::cerr << "Failed to create MMF" << std::endl;
        return 1;
    }

#ifdef _WIN32
    child1 = ProcessCreateWithMMF("child1.exe", "parent_to_child1", "child1_to_child2"
        );
    child2 = ProcessCreateWithMMF("child2.exe", "child1_to_child2", "child2_to_parent"
        );
#else
    child1 = ProcessCreateWithMMF("./child1", "parent_to_child1", "child1_to_child2");
    child2 = ProcessCreateWithMMF("./child2", "child1_to_child2", "child2_to_parent");
#endif

    if (!child1.is_valid || !child2.is_valid) {
        std::cerr << "Failed to create child processes" << std::endl;
        MMFClose(&mmf1);
        MMFClose(&mmf2);
        MMFClose(&mmf3);
        return 1;
    }

#ifdef _WIN32
    Sleep(500);
#else
    usleep(500000);
#endif

    std::cout << "Ready. Enter strings (empty line to exit):" << std::endl;

    std::string input;
    while (true) {
        std::cout << "> ";
        std::getline(std::cin, input);

        if (input.empty()) {
            break;
        }

        if (WriteToMMF(mmf1, input)) {
            std::cout << "Sent to child1: " << input << std::endl;

            bool data_ready = false;
            int attempts = 0;
            while (!data_ready && attempts < 100) {
                std::string result = ReadFromMMF(mmf3);
                if (!result.empty()) {
                    std::cout << "Result: " << result << std::endl;
                    ClearMMF(mmf3);
                    data_ready = true;
                }
                attempts++;
            }

            if (!data_ready) {
                std::cerr << "Timeout waiting for result" << std::endl;
            }
            ClearMMF(mmf1);
        } else {
            std::cerr << "Failed to send data" << std::endl;
        }
    }

    if (child1.is_valid) {
        ProcessTerminate(&child1);
    }
    if (child2.is_valid) {
        ProcessTerminate(&child2);
    }

    MMFClose(&mmf1);
    MMFClose(&mmf2);
    MMFClose(&mmf3);

    std::cout << "Program finished" << std::endl;
    return 0;
}
```

child1.cpp

```
#include <iostream>
#include <string>
#include <algorithm>
#include <cctype>

```

```
#include "systemCall.h"

int main(int argc, char* argv[]) {
    const char* input_mmf_name = argc > 1 ? argv[1] : "parent_to_child1";
    const char* output_mmf_name = argc > 2 ? argv[2] : "child1_to_child2";

    mmfT input_mmf, output_mmf;
    input_mmf.handle = INVALID_MMF_HANDLE; input_mmf.data = nullptr;
    output_mmf.handle = INVALID_MMF_HANDLE; output_mmf.data = nullptr;

    if (!MMFOpen(&input_mmf, input_mmf_name, 1024) ||
        !MMFOpen(&output_mmf, output_mmf_name, 1024)) {
        std::cerr << "Child1: Failed to open MMF" << std::endl;
        return 1;
    }

    while (true) {
        std::string data = ReadFromMMF(input_mmf);

        if (!data.empty()) {
            std::string processed_data = data;
            std::transform(processed_data.begin(), processed_data.end(),
                          processed_data.begin(),
                          [](unsigned char c){ return std::tolower(c); });

            if (WriteToMMF(output_mmf, processed_data)) {
                ClearMMF(input_mmf);
            }
        }
    }

    return 0;
}
```

child2.cpp

```
#include <iostream>
#include <string>
#include <cctype>

#include "systemCall.h"

int main(int argc, char* argv[]) {
    const char* input_mmf_name = argc > 1 ? argv[1] : "child1_to_child2";
    const char* output_mmf_name = argc > 2 ? argv[2] : "child2_to_parent";

    mmfT input_mmf, output_mmf;
    input_mmf.handle = INVALID_MMF_HANDLE; input_mmf.data = nullptr;
    output_mmf.handle = INVALID_MMF_HANDLE; output_mmf.data = nullptr;

    if (!MMFOpen(&input_mmf, input_mmf_name, 1024) ||
        !MMFOpen(&output_mmf, output_mmf_name, 1024)) {
        std::cerr << "Child2: Failed to open MMF" << std::endl;
        return 1;
    }

    while (true) {
        std::string data = ReadFromMMF(input_mmf);

        if (!data.empty()) {
            std::string result;
            bool prev_space = false;

            for (char c : data) {
                if (std::isspace(c)) {
                    if (!prev_space) {
                        result += c;
                        prev_space = true;
                    }
                } else {
                    result += c;
                    prev_space = false;
                }
            }

            if (WriteToMMF(output_mmf, result)) {
                ClearMMF(input_mmf);
            }
        }
    }

    return 0;
}
```

strace

```
"Time of Day","Process Name","PID","Operation","Path","Result","Detail"
"23:43:40,6503020","parent.exe","20288","Process Start","","SUCCESS","Parent
PID: 18420,Command line: ""C:\Users\kseni\lab3OSWaL\lab3OS\build\bin\parent.exe"",Cur
directory: C:\Users\kseni\lab3OSWaL\lab3OS\build\,Environment:
; ALLUSERSPROFILE=C:\ProgramData
; APPDATA=C:\Users\kseni\AppData\Roaming
; CC=C:/Users/kseni/gcc/bin/gcc.exe
; CHROME_CRASHPAD_PIPE_NAME=\\.\pipe\crashpad_8816_YEISNMMSRDSWYGZY
; CommonProgramFiles=C:\Program Files\Common Files
; CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
; CommonProgramW6432=C:\Program Files\Common Files
; COMPUTERNAME=LAPTOP-ECH40E5U
; ComSpec=C:\Windows\system32\cmd.exe
; CXX=C:/Users/kseni/gcc/bin/g++.exe
; DriverData=C:\Windows\System32\Drivers\DriverData
; EFC_4556=1
; HOMEDRIVE=C:
; HOMEPATH=\Users\kseni
; JAVA_HOME=C:\Program Files\Zulu\zulu-17\
; LOCALAPPDATA=C:\Users\kseni\AppData\Local
; LOGONSERVER=\\LAPTOP-ECH40E5U
; NUMBER_OF_PROCESSORS=8
; OneDrive=C:\Users\kseni\OneDrive
; OneDriveConsumer=C:\Users\kseni\OneDrive
; ORIGINAL_XDG_CURRENT_DESKTOP=undefined
; OS=Windows_NT
; Path=D:\Program Files\VMware\VMware Workstation\bin\;%PATH%;C:/Users/kseni/gcc/bin;
Files\swipl\bin;C:\Program Files\Git\bin;D:\Program Files\VMware\VMware Workstation\b
Files\swipl\bin;C:/Users/kseni/gcc/bin;;C:\Users\kseni\AppData\Local\Programs\Microso
VS Code\bin;C:\Program Files\CMake\bin
; PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.CPL
; PROCESSOR_ARCHITECTURE=AMD64
; PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 140 Stepping 2,GenuineIntel
; PROCESSOR_LEVEL=6
; PROCESSOR_REVISION=8c02
; ProgramData=C:\ProgramData
; ProgramFiles=C:\Program Files
; ProgramFiles(x86)=C:\Program Files (x86)
; ProgramW6432=C:\Program Files
; PSModulePath=C:\Users\kseni\OneDrive\Документы\WindowsPowerShell\Modules;C:\Program
Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
; PUBLIC=C:\Users\Public
; PyCharm Community Edition=C:\Program Files\JetBrains\PyCharm Community Edition
2023.3.3\bin;
; SESSIONNAME=Console
; SystemDrive=C:
; SystemRoot=C:\Windows
; TEMP=C:\Users\kseni\AppData\Local\Temp
; TMP=C:\Users\kseni\AppData\Local\Temp
; USERDOMAIN=LAPTOP-ECH40E5U
; USERDOMAIN_ROAMINGPROFILE=LAPTOP-ECH40E5U
; USERNAME=kseni
; USERPROFILE=C:\Users\kseni
; windir=C:\Windows
; ZES_ENABLE_SYSMAN=1
; TERM_PROGRAM=vscode
; TERM_PROGRAM_VERSION=1.106.2
; LANG=en_US.UTF-8
; COLORTERM=truecolor
; GIT_ASKPASS=c:\Users\kseni\AppData\Local\Programs\Microsoft VS Code\resources\app\e
; VSCODE_GIT_ASKPASS_NODE=C:\Users\kseni\AppData\Local\Programs\Microsoft VS
Code\Code.exe
; VSCODE_GIT_ASKPASS_EXTRA_ARGS=
; VSCODE_GIT_ASKPASS_MAIN=c:\Users\kseni\AppData\Local\Programs\Microsoft VS
Code\resources\app\extensions\git\dist\askpass-main.js
; VSCODE_GIT_IPC_HANDLE=\\.\pipe\vscode-git-c7bf6ff4a2-sock
; VSCODE_INJECTION=1
; VSCODE_NONCE=43b5c285-35e7-4e28-8228-2d43d27bea9e
; VSCODE_A11Y_MODE=0
; VSCODE_STABLE=1"
"23:43:40,6503115","parent.exe","20288","Thread Create","","SUCCESS","Thread
ID: 20272"
"23:43:40,6563945","parent.exe","20288","Load Image","C:\Users\kseni\lab3OSWaL\lab3OS
Base: 0x7ff60a250000,Image Size: 0xd8f000"
```

```
"23:43:40,6564545","parent.exe","20288","Load Image","C:\Windows\System32\ntdll.dll",
Base: 0x7ffbdceb0000,Image Size: 0x217000"
"23:43:40,6565665","parent.exe","20288","CreateFile","C:\Windows\Prefetch\PARENT.EXE-
NOT FOUND","Desired Access: Generic Read,Disposition: Open,Options: Synchronous
IO Non-Alert,Attributes: n/a,ShareMode: None,AllocationSize: n/a"
"23:43:40,6567210","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Read"
"23:43:40,6567405","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Read"
"23:43:40,6567567","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
REG_SZ,Length: 10,Data: 1251"
"23:43:40,6567757","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
REG_SZ,Length: 8,Data: 866"
"23:43:40,6567911","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
"23:43:40,6568722","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager","REPARSE","Desired Access: Query Value"
"23:43:40,6568835","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager","SUCCESS","Desired Access: Query Value"
"23:43:40,6568951","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
Manager\RaiseExceptionOnPossibleDeadlock","NAME NOT FOUND","Length: 80"
"23:43:40,6569050","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
Manager","SUCCESS",""
"23:43:40,6569148","parent.exe","20288","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\C
Manager\Segment Heap","REPARSE","Desired Access: Query Value"
"23:43:40,6569240","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager\Segment Heap","NAME NOT FOUND","Desired Access: Query Value"
"23:43:40,6569589","parent.exe","20288","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\C
Manager","REPARSE","Desired Access: Query Value,Enumerate Sub Keys"
"23:43:40,6569673","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager","SUCCESS","Desired Access: Query Value,Enumerate Sub Keys"
"23:43:40,6569756","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
Manager\ResourcePolicies","NAME NOT FOUND","Length: 24"
"23:43:40,6569841","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
Manager","SUCCESS",""
"23:43:40,6571155","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 528"
"23:43:40,6571579","parent.exe","20288","QueryNameInformationFile","C:\Windows\System
\Windows\System32\ntdll.dll"
"23:43:40,6572063","parent.exe","20288","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\C
Manager","REPARSE","Desired Access: Query Value,Enumerate Sub Keys"
"23:43:40,6572172","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager","SUCCESS","Desired Access: Query Value,Enumerate Sub Keys"
"23:43:40,6572271","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
Manager\ResourcePolicies","NAME NOT FOUND","Length: 24"
"23:43:40,6572369","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
Manager","SUCCESS",""
"23:43:40,6574310","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Execute/Traverse,Synchronize,Disposition: Open,Options: Directory,Synchronous
```

```
IO Non-Alert,Attributes: n/a,ShareMode: Read,Write,AllocationSize: n/a,OpenResult:
Opened"
"23:43:40,6575446","parent.exe","20288","Load Image","C:\Windows\System32\kernel32.dl
Base: 0x7ffbdbaf0000,Image Size: 0xc4000"
"23:43:40,6578340","parent.exe","20288","Load Image","C:\Windows\System32\KernelBase.
Base: 0x7ffbda680000,Image Size: 0x3b7000"
"23:43:40,6589143","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 528"
"23:43:40,6589725","parent.exe","20288","QueryNameInformationFile","C:\Windows\System
\Windows\System32\KernelBase.dll"
"23:43:40,6591715","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 528"
"23:43:40,6592307","parent.exe","20288","QueryNameInformationFile","C:\Windows\System
\Windows\System32\KernelBase.dll"
"23:43:40,6594010","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Read"
"23:43:40,6594226","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
NOT FOUND","Desired Access: Read"
"23:43:40,6594899","parent.exe","20288","QueryNameInformationFile","C:\Windows\System
\Windows\System32\KernelBase.dll"
"23:43:40,6595215","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 528"
"23:43:40,6595566","parent.exe","20288","QueryNameInformationFile","C:\Windows\System
\Windows\System32\KernelBase.dll"
"23:43:40,6596031","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Server","REPARSE","Desired Access: Read"
"23:43:40,6596186","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Server","SUCCESS","Desired Access: Read"
"23:43:40,6596357","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
Server\TSAppCompat","NAME NOT FOUND","Length: 548"
"23:43:40,6596482","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
Server\TSUserEnabled","SUCCESS","Type: REG_DWORD,Length: 4,Data: 0"
"23:43:40,6596648","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
Server","SUCCESS",""
"23:43:40,6598585","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Query Value,Set Value"
"23:43:40,6598731","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
NOT FOUND","Desired Access: Query Value,Set Value"
"23:43:40,6598892","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Read"
"23:43:40,6599017","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Read"
"23:43:40,6599192","parent.exe","20288","RegQueryKey","HKLM\System\CurrentControlSet\
Full,SubKeys: 1,Values: 0"
"23:43:40,6599347","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
"23:43:40,6599471","parent.exe","20288","RegOpenKey","HKLM\Software\Policies\Microsof
Access: Query Value"
"23:43:40,6599673","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Policies\Micro
```

```
NOT FOUND","Length: 80"
"23:43:40,6599816","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Policies\Microso
"23:43:40,6599972","parent.exe","20288","RegOpenKey","HKCU\Software\Policies\Microsof
NOT FOUND","Desired Access: Query Value"
"23:43:40,6600249","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Read"
"23:43:40,6600378","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Read"
"23:43:40,6600512","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
REG_DWORD,Length: 4,Data: 1"
"23:43:40,6600677","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 20"
"23:43:40,6600806","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
"23:43:40,6602750","parent.exe","20288","CreateFile","C:\Windows\System32\apphelp.dll
Access: Read Attributes,Disposition: Open,Options: Open Reparse Point,Attributes:
n/a,ShareMode: Read,Write,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6603168","parent.exe","20288","QueryBasicInformationFile","C:\Windows\Syste
15.07.2024 15:21:56,LastAccessTime: 20.11.2025 23:43:26,LastWriteTime: 15.07.2024
15:21:56,ChangeTime: 16.10.2024 21:20:32,FileAttributes: A"
"23:43:40,6603321","parent.exe","20288","CloseFile","C:\Windows\System32\apphelp.dll"
"23:43:40,6604226","parent.exe","20288","CreateFile","C:\Windows\System32\apphelp.dll
Access: Read Data/List Directory,Execute/Traverse,Synchronize,Disposition:
Open,Options: Synchronous IO Non-Alert,Non-Directory File,Attributes: n/a,ShareMode:
Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6604739","parent.exe","20288","CreateFileMapping","C:\Windows\System32\apph
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READ|PAGE_NOCACHE"
"23:43:40,6605048","parent.exe","20288","CreateFileMapping","C:\Windows\System32\apph
SyncTypeOther"
"23:43:40,6605307","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Read"
"23:43:40,6605465","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Read"
"23:43:40,6605633","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
REG_DWORD,Length: 4,Data: 2"
"23:43:40,6605777","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
"23:43:40,6608448","parent.exe","20288","Load Image","C:\Windows\System32\apphelp.dll
Base: 0x7ffbd54f0000,Image Size: 0x97000"
"23:43:40,6610167","parent.exe","20288","CloseFile","C:\Windows\System32\apphelp.dll"
"23:43:40,6611137","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 528"
"23:43:40,6611662","parent.exe","20288","QueryNameInformationFile","C:\Windows\System
\Windows\System32\apphelp.dll"
"23:43:40,6612371","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags","SUCCESS","Desired Access: Query Value"
"23:43:40,6612636","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\LogFlags","NAME NOT FOUND","Length: 20"
"23:43:40,6612806","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
```

```
NT\CurrentVersion\AppCompatFlags","SUCCESS",""
"23:43:40,6613002","parent.exe","20288","RegOpenKey","HKLM\OSDATA\Software\Microsoft\
NT\CurrentVersion\AppCompatFlags","NAME NOT FOUND","Desired Access: Query Value"
"23:43:40,6613586","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 528"
"23:43:40,6614027","parent.exe","20288","QueryNameInformationFile","C:\Windows\System
\Windows\System32\apphelp.dll"
"23:43:40,6614958","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags","SUCCESS","Desired Access: Query Value"
"23:43:40,6615149","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\ShowDebugInfo","NAME NOT FOUND","Length: 20"
"23:43:40,6615306","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags","SUCCESS",""
"23:43:40,6616237","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Read Control,Disposition: Open,Options: ,Attributes: n/a,ShareMode:
Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6616520","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
OVERFLOW","Information: Owner"
"23:43:40,6616657","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Owner"
"23:43:40,6616800","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6618489","parent.exe","20288","CreateFile","C:\Windows\System32\ntdll.dll",
Access: Read Control,Disposition: Open,Options: ,Attributes: n/a,ShareMode:
Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6618950","parent.exe","20288","QuerySecurityFile","C:\Windows\System32\ntdl
OVERFLOW","Information: Owner"
"23:43:40,6619102","parent.exe","20288","QuerySecurityFile","C:\Windows\System32\ntdl
Owner"
"23:43:40,6619287","parent.exe","20288","CloseFile","C:\Windows\System32\ntdll.dll","
"23:43:40,6620383","parent.exe","20288","CreateFile","C:\Windows\System32\kernel32.dl
Access: Read Control,Disposition: Open,Options: ,Attributes: n/a,ShareMode:
Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6620679","parent.exe","20288","QuerySecurityFile","C:\Windows\System32\kern
OVERFLOW","Information: Owner"
"23:43:40,6620764","parent.exe","20288","QuerySecurityFile","C:\Windows\System32\kern
Owner"
"23:43:40,6620851","parent.exe","20288","CloseFile","C:\Windows\System32\kernel32.dll
"23:43:40,6621536","parent.exe","20288","CreateFile","C:\Windows\System32\KernelBase.
Access: Read Control,Disposition: Open,Options: ,Attributes: n/a,ShareMode:
Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6621700","parent.exe","20288","QuerySecurityFile","C:\Windows\System32\Kern
OVERFLOW","Information: Owner"
"23:43:40,6621776","parent.exe","20288","QuerySecurityFile","C:\Windows\System32\Kern
Owner"
"23:43:40,6621858","parent.exe","20288","CloseFile","C:\Windows\System32\KernelBase.d
"23:43:40,6622249","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6622437","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
```

```
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysmain.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6622547","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6623242","parent.exe","20288","CreateFile","C:\Windows\apppatch\sysmain.sdb
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6623735","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6623875","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6624061","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\sysm
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READ|PAGE_NOCACHE"
"23:43:40,6624218","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6624485","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\sysm
SyncTypeOther"
"23:43:40,6625021","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6625234","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\DisableDoubleQuerySdbs","NAME NOT
FOUND","Length: 20"
"23:43:40,6625384","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6625542","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Desir
Access: Read"
"23:43:40,6625732","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ,Length: 24,Data: sysmain.sdb"
"23:43:40,6625883","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ"
"23:43:40,6626035","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS",""
"23:43:40,6626202","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6626359","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6626487","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6626685","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
```

```
"23:43:40,6626826","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6626940","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6627663","parent.exe","20288","CreateFile","C:\Windows\apppatch\MergeSdbFil
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6628151","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6628275","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6628421","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\Merg
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READ|PAGE_NOCACHE"
"23:43:40,6628568","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6628833","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\Merg
SyncTypeOther"
"23:43:40,6630771","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6631270","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
Folders","SUCCESS","Desired Access: Query Value"
"23:43:40,6631518","parent.exe","20288","RegQueryValue","HKCU\Software\Microsoft\Wind
Folders\Cache","SUCCESS","Type: REG_SZ,Length: 114,Data: C:\Users\kseni\AppData\Local
"23:43:40,6631756","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
Folders","SUCCESS",""
"23:43:40,6631997","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Owner,Group,DACL,SACL,Label,Attribute,Process Trust Label,0x100"
"23:43:40,6632430","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6632661","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\DisableDoubleQuerySdbs","NAME NOT
FOUND","Length: 20"
"23:43:40,6632841","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6633016","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Desir
Access: Read"
"23:43:40,6633221","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ,Length: 24,Data: sysmain.sdb"
"23:43:40,6633399","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ"
"23:43:40,6633592","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS",""
```

```
"23:43:40,6633775","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6633965","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6634133","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6634493","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6634684","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysmain.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6634873","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6635002","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:09,LastAccessTime: 20.11.2025 23:43:40,LastWriteTime: 20.11.2025
23:32:24,ChangeTime: 20.11.2025 23:32:24,FileAttributes: A"
"23:43:40,6635293","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6636402","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6636876","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
Folders","SUCCESS","Desired Access: Query Value"
"23:43:40,6637085","parent.exe","20288","RegQueryValue","HKCU\Software\Microsoft\Windo
Folders\Cache","SUCCESS","Type: REG_SZ,Length: 114,Data: C:\Users\kseni\AppData\Local
"23:43:40,6637237","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
Folders","SUCCESS",""
"23:43:40,6637434","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Owner,Group,DACL,SACL,Label,Attribute,Process Trust Label,0x100"
"23:43:40,6637584","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:09,LastAccessTime: 20.11.2025 23:43:40,LastWriteTime: 20.11.2025
23:32:24,ChangeTime: 20.11.2025 23:32:24,FileAttributes: A"
"23:43:40,6637771","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6640215","parent.exe","20288","CloseFile","C:\Windows\apppatch\sysmain.sdb"
"23:43:40,6641021","parent.exe","20288","CloseFile","C:\Windows\apppatch\MergeSdbFile
"23:43:40,6643651","parent.exe","20288","Load Image","C:\Windows\System32\msvcrt.dll"
Base: 0x7ffbdbc20000,Image Size: 0xa7000"
"23:43:40,6644809","parent.exe","20288","Thread Create","","SUCCESS","Thread
ID: 19752"
"23:43:40,6648342","parent.exe","20288","CreateFile","C:\Windows\System32\msvcrt.dll"
Access: Read Control,Disposition: Open,Options: ,Attributes: n/a,ShareMode:
Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6648737","parent.exe","20288","QuerySecurityFile","C:\Windows\System32\msvc
OVERFLOW","Information: Owner"
"23:43:40,6648884","parent.exe","20288","QuerySecurityFile","C:\Windows\System32\msvc
Owner"
"23:43:40,6649038","parent.exe","20288","CloseFile","C:\Windows\System32\msvcrt.dll",
"23:43:40,6651377","parent.exe","20288","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\C
```

```
Manager","REPARSE","Desired Access: Query Value,Enumerate Sub Keys"
"23:43:40,6651706","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager","SUCCESS","Desired Access: Query Value,Enumerate Sub Keys"
"23:43:40,6651947","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
Manager\ResourcePolicies","NAME NOT FOUND","Length: 24"
"23:43:40,6652133","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
Manager","SUCCESS",""
"23:43:40,6652771","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Read"
"23:43:40,6652936","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Read"
"23:43:40,6653135","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
REG_SZ,Length: 18,Data: 00060403"
"23:43:40,6653305","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
REG_SZ,Length: 26,Data: kernel32.dll"
"23:43:40,6653950","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager","REPARSE","Desired Access: Query Value"
"23:43:40,6654043","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager","SUCCESS","Desired Access: Query Value"
"23:43:40,6654151","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
Manager\SmtDelaySleepLoopWindowSize","NAME NOT FOUND","Length: 80"
"23:43:40,6654227","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
Manager\SmtDelaySpinCountThreshold","NAME NOT FOUND","Length: 80"
"23:43:40,6654298","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
Manager\SmtDelayBaseYield","NAME NOT FOUND","Length: 80"
"23:43:40,6654369","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
Manager\SmtFactorYield","NAME NOT FOUND","Length: 80"
"23:43:40,6654435","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
Manager\SmtDelayMaxYield","NAME NOT FOUND","Length: 80"
"23:43:40,6654552","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
Manager","SUCCESS",""
"23:43:40,6655241","parent.exe","20288","QueryNameInformationFile","C:\Users\kseni\la
\Users\kseni\lab1OSLinuxToWind\lab3OS\build\bin\parent.exe"
"23:43:40,6696331","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Read Attributes,Disposition: Open,Options: Open Reparse Point,Attributes:
n/a,ShareMode: Read,Write,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6696676","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:15,LastAccessTime: 20.11.2025 23:39:09,LastWriteTime: 20.11.2025
23:23:34,ChangeTime: 20.11.2025 23:23:34,FileAttributes: A"
"23:43:40,6696800","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6697922","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Read Attributes,Disposition: Open,Options: Open Reparse Point,Attributes:
n/a,ShareMode: Read,Write,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6698065","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:15,LastAccessTime: 20.11.2025 23:39:09,LastWriteTime: 20.11.2025
23:23:34,ChangeTime: 20.11.2025 23:23:34,FileAttributes: A"
"23:43:40,6698150","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6699217","parent.exe","20288","Load Image","C:\Windows\System32\sechost.dll
```

```
Base: 0x7ffbdba40000,Image Size: 0xa8000"
"23:43:40,6700569","parent.exe","20288","Load Image","C:\Windows\System32\bcrypt.dll"
Base: 0x7ffbdabb0000,Image Size: 0x28000"
"23:43:40,6701619","parent.exe","20288","Thread Create","","SUCCESS","Thread
ID: 20352"
"23:43:40,6703052","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 528"
"23:43:40,6703661","parent.exe","20288","QueryNameInformationFile","C:\Windows\System
\Windows\System32\bcrypt.dll"
"23:43:40,6705135","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 528"
"23:43:40,6705518","parent.exe","20288","QueryNameInformationFile","C:\Windows\System
\Windows\System32\sechost.dll"
"23:43:40,6705854","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 528"
"23:43:40,6706135","parent.exe","20288","QueryNameInformationFile","C:\Windows\System
\Windows\System32\sechost.dll"
"23:43:40,6706723","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options","SUCCESS","Desired Access:
Query Value,Enumerate Sub Keys"
"23:43:40,6706935","parent.exe","20288","RegOpenKey","HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\child1.exe","NAME NOT FOUND","Desired
Access: Query Value,Enumerate Sub Keys"
"23:43:40,6707088","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Wow64\x
NOT FOUND","Desired Access: Query Value"
"23:43:40,6707927","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Read Data/List Directory,Execute/Traverse,Read Attributes,Synchronize,Disposi
Open,Options: Synchronous IO Non-Alert,Non-Directory File,Attributes: N,ShareMode:
Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6708275","parent.exe","20288","CreateFileMapping","C:\Users\kseni\lab3OSWaL
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
"
"23:43:40,6708468","parent.exe","20288","CreateFileMapping","C:\Users\kseni\lab3OSWaL
SyncTypeOther"
"23:43:40,6708787","parent.exe","20288","RegOpenKey","HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\child1.exe","NAME NOT FOUND","Desired
Access: Query Value,Enumerate Sub Keys"
"23:43:40,6709014","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Label"
"23:43:40,6709561","parent.exe","20288","QueryNameInformationFile","C:\Users\kseni\la
\Users\kseni\lab3OSWaL\lab3OS\build\bin\child1.exe"
"23:43:40,6732732","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\S
Access: All Access"
"23:43:40,6733574","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 40"
"23:43:40,6733801","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
"23:43:40,6734002","parent.exe","20288","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\C
Manager\BAM","REPARSE","Desired Access: Query Value"
```

```
"23:43:40,6734175","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager\BAM","NAME NOT FOUND","Desired Access: Query Value"
"23:43:40,6734533","parent.exe","20288","Process Create","C:\Users\kseni\lab3OSWaL\la
20304,Command line: child1.exe parent_to_child1 child1_to_child2"
"23:43:40,6735017","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager\AppCertDlls","REPARSE","Desired Access: Query Value"
"23:43:40,6735140","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager\AppCertDlls","NAME NOT FOUND","Desired Access: Query Value"
"23:43:40,6735329","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Access: Query Value,Set Value"
"23:43:40,6735435","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
NOT FOUND","Desired Access: Query Value,Set Value"
"23:43:40,6735556","parent.exe","20288","RegOpenKey","HKLM\Software\Policies\Microsof
Access: Query Value"
"23:43:40,6735751","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Policies\Micro
NOT FOUND","Length: 80"
"23:43:40,6735832","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Policies\Micro
REG_DWORD,Length: 4,Data: 0"
"23:43:40,6735917","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Policies\Microso
"23:43:40,6736021","parent.exe","20288","RegOpenKey","HKCU\Software\Policies\Microsof
NOT FOUND","Desired Access: Query Value"
"23:43:40,6736543","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
Folders","SUCCESS","Desired Access: Query Value"
"23:43:40,6736664","parent.exe","20288","RegQueryValue","HKCU\Software\Microsoft\Wind
Folders\Cache","SUCCESS","Type: REG_SZ,Length: 114,Data: C:\Users\kseni\AppData\Local
"23:43:40,6736784","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
Folders","SUCCESS",""
"23:43:40,6736874","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
NT\CurrentVersion","SUCCESS","Desired Access: Enumerate Sub Keys"
"23:43:40,6736967","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS","Desired Access: Query Value"
"23:43:40,6737056","parent.exe","20288","RegQueryValue","HKCU\Software\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\kseni\lab3OSWaL\lab3OS\build\bin\chi
NOT FOUND","Length: 16"
"23:43:40,6737130","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS",""
"23:43:40,6737325","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Owner,Group,DACL,SACL,Label,Attribute,Process Trust Label,0x100"
"23:43:40,6737666","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6737824","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\DisableDoubleQuerySdbs","NAME NOT
FOUND","Length: 20"
"23:43:40,6737918","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6738004","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Desir
Access: Read"
```

```
"23:43:40,6738120","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ,Length: 24,Data: sysmain.sdb"
"23:43:40,6738211","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ"
"23:43:40,6738306","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS",""
"23:43:40,6738389","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6738482","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6738559","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6738713","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6738796","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysmain.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6738871","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6738967","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:15,LastAccessTime: 20.11.2025 23:39:09,LastWriteTime: 20.11.2025
23:23:34,ChangeTime: 20.11.2025 23:23:34,FileAttributes: A"
"23:43:40,6739772","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:15,LastAccessTime: 20.11.2025 23:39:09,LastWriteTime: 20.11.2025
23:23:34,ChangeTime: 20.11.2025 23:23:34,FileAttributes: A"
"23:43:40,6739868","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Owner"
"23:43:40,6740012","parent.exe","20288","QueryNameInformationFile","C:\Users\kseni\la
\Users\kseni\lab3OSWaL\lab3OS\build\bin\child1.exe"
"23:43:40,6740505","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6740599","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysmain.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6740684","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6741298","parent.exe","20288","CreateFile","C:\Windows\apppatch\sysmain.sdb
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6741650","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6741733","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
```

```
"23:43:40,6741845","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\sysma
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READWRITE"
"23:43:40,6741951","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6742143","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\sysma
SyncTypeOther"
"23:43:40,6742504","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6742614","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\DisableDoubleQuerySdbs","NAME NOT
FOUND","Length: 20"
"23:43:40,6742705","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6742792","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Desir
Access: Read"
"23:43:40,6742897","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ,Length: 24,Data: sysmain.sdb"
"23:43:40,6742978","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ"
"23:43:40,6743067","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS",""
"23:43:40,6743170","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6743256","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6743335","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6743446","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6743526","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6743601","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6744072","parent.exe","20288","CreateFile","C:\Windows\apppatch\MergeSdbFil
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6744353","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6744427","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6744527","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\Merg
```

```
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READWRITE"
"23:43:40,6744629","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6744809","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\Merg
SyncTypeOther"
"23:43:40,6745049","parent.exe","20288","QueryStandardInformationFile","C:\Users\ksen
15 917 056,EndOfFile: 15 913 317,NumberOfLinks: 1,DeletePending: False,Directory:
False"
"23:43:40,6745195","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS","Desired Access: Read"
"23:43:40,6745312","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\kseni\lab3OSWaL\lab3OS\build\bin\chi
NOT FOUND","Length: 1 024"
"23:43:40,6745408","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS",""
"23:43:40,6745519","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS","Desired Access: Read"
"23:43:40,6745633","parent.exe","20288","RegQueryValue","HKCU\Software\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\kseni\lab3OSWaL\lab3OS\build\bin\chi
NOT FOUND","Length: 1 024"
"23:43:40,6745724","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS",""
"23:43:40,6745813","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Custom\child1.exe","NAME NOT FOUND","Desired
Access: Read"
"23:43:40,6746799","parent.exe","20288","QueryStandardInformationFile","C:\Users\ksen
15 917 056,EndOfFile: 15 913 317,NumberOfLinks: 1,DeletePending: False,Directory:
False"
"23:43:40,6746901","parent.exe","20288","CreateFileMapping","C:\Users\kseni\lab3OSWaL
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READ|PAGE_NOCACHE"
"23:43:40,6746997","parent.exe","20288","QueryStandardInformationFile","C:\Users\ksen
15 917 056,EndOfFile: 15 913 317,NumberOfLinks: 1,DeletePending: False,Directory:
False"
"23:43:40,6747189","parent.exe","20288","CreateFileMapping","C:\Users\kseni\lab3OSWaL
SyncTypeOther"
"23:43:40,6756390","parent.exe","20288","CloseFile","C:\Windows\apppatch\sysmain.sdb"
"23:43:40,6757187","parent.exe","20288","CloseFile","C:\Windows\apppatch\MergeSdbFile
"23:43:40,6757711","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:15,LastAccessTime: 20.11.2025 23:39:09,LastWriteTime: 20.11.2025
23:23:34,ChangeTime: 20.11.2025 23:23:34,FileAttributes: A"
"23:43:40,6758040","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
Access: Read"
"23:43:40,6758252","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NOT FOUND","Length: 20"
"23:43:40,6758389","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
"23:43:40,6758818","parent.exe","20288","RegOpenKey","HKCU","SUCCESS","Desired
```

```
Access: Maximum Allowed,Granted Access: All Access"
"23:43:40,6758952","parent.exe","20288","RegOpenKey","HKCU\Control Panel\Desktop\MuiC
NOT FOUND","Desired Access: Read"
"23:43:40,6759089","parent.exe","20288","RegCloseKey","HKCU","SUCCESS",""
"23:43:40,6759182","parent.exe","20288","RegOpenKey","HKLM\Software\Policies\Microsof
NOT FOUND","Desired Access: Read"
"23:43:40,6759327","parent.exe","20288","RegOpenKey","HKCU","SUCCESS","Desired
Access: Maximum Allowed,Granted Access: All Access"
"23:43:40,6759429","parent.exe","20288","RegOpenKey","HKCU\Software\Policies\Microsof
Panel\Desktop","NAME NOT FOUND","Desired Access: Read"
"23:43:40,6759538","parent.exe","20288","RegOpenKey","HKCU\Control Panel\Desktop\Lang
NOT FOUND","Desired Access: Read"
"23:43:40,6759640","parent.exe","20288","RegCloseKey","HKCU","SUCCESS",""
"23:43:40,6759733","parent.exe","20288","RegOpenKey","HKLM\Software\Policies\Microsof
NOT FOUND","Desired Access: Read"
"23:43:40,6759839","parent.exe","20288","RegOpenKey","HKCU","SUCCESS","Desired
Access: Maximum Allowed,Granted Access: All Access"
"23:43:40,6759943","parent.exe","20288","RegOpenKey","HKCU\Software\Policies\Microsof
Panel\Desktop","NAME NOT FOUND","Desired Access: Read"
"23:43:40,6760037","parent.exe","20288","RegOpenKey","HKCU\Control Panel\Desktop","SU
Access: Read"
"23:43:40,6760148","parent.exe","20288","RegQueryValue","HKCU\Control Panel\Desktop\P
NOT FOUND","Length: 12"
"23:43:40,6760258","parent.exe","20288","RegCloseKey","HKCU\Control Panel\Desktop","S
"23:43:40,6760339","parent.exe","20288","RegCloseKey","HKCU","SUCCESS",""
"23:43:40,6760423","parent.exe","20288","RegOpenKey","HKLM\Software\Policies\Microsof
NOT FOUND","Desired Access: Read"
"23:43:40,6760527","parent.exe","20288","RegOpenKey","HKCU","SUCCESS","Desired
Access: Maximum Allowed,Granted Access: All Access"
"23:43:40,6760626","parent.exe","20288","RegOpenKey","HKCU\Control Panel\Desktop\MuiC
Access: Read"
"23:43:40,6760727","parent.exe","20288","RegQueryValue","HKCU\Control Panel\Desktop\M
OVERFLOW","Length: 12"
"23:43:40,6760871","parent.exe","20288","RegQueryValue","HKCU\Control Panel\Desktop\M
REG_MULTI_SZ,Length: 12,Data: ru-RU"
"23:43:40,6761051","parent.exe","20288","RegCloseKey","HKCU\Control Panel\Desktop\Mui
"23:43:40,6761189","parent.exe","20288","RegCloseKey","HKCU","SUCCESS",""
"23:43:40,6761305","parent.exe","20288","RegOpenKey","HKLM\Software\Policies\Microsof
NOT FOUND","Desired Access: Read"
"23:43:40,6761414","parent.exe","20288","RegOpenKey","HKCU","SUCCESS","Desired
Access: Maximum Allowed,Granted Access: All Access"
"23:43:40,6761518","parent.exe","20288","RegOpenKey","HKCU\Software\Policies\Microsof
Panel\Desktop","NAME NOT FOUND","Desired Access: Read"
"23:43:40,6761610","parent.exe","20288","RegOpenKey","HKCU\Control Panel\Desktop","SU
Access: Read"
"23:43:40,6761703","parent.exe","20288","RegQueryValue","HKCU\Control Panel\Desktop\P
NOT FOUND","Length: 12"
"23:43:40,6761803","parent.exe","20288","RegCloseKey","HKCU\Control Panel\Desktop","S
```

```
"23:43:40,6761882","parent.exe","20288","RegCloseKey","HKCU","SUCCESS",""
"23:43:40,6761983","parent.exe","20288","RegOpenKey","HKLM\Software\Policies\Microsof
NOT FOUND","Desired Access: Read"
"23:43:40,6762113","parent.exe","20288","RegOpenKey","HKCU","SUCCESS","Desired
Access: Maximum Allowed,Granted Access: All Access"
"23:43:40,6762212","parent.exe","20288","RegOpenKey","HKCU\Software\Policies\Microsof
Panel\Desktop","NAME NOT FOUND","Desired Access: Read"
"23:43:40,6762308","parent.exe","20288","RegOpenKey","HKCU\Control Panel\Desktop\Lang
NOT FOUND","Desired Access: Read"
"23:43:40,6762399","parent.exe","20288","RegCloseKey","HKCU","SUCCESS",""
"23:43:40,6785324","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
Folders","SUCCESS","Desired Access: Query Value"
"23:43:40,6785669","parent.exe","20288","RegQueryValue","HKCU\Software\Microsoft\Wind
Folders\Cache","SUCCESS","Type: REG_SZ,Length: 114,Data: C:\Users\kseni\AppData\Local
"23:43:40,6785931","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
Folders","SUCCESS",""
"23:43:40,6786249","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Owner,Group,DACL,SACL,Label,Attribute,Process Trust Label,0x100"
"23:43:40,6786837","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6787102","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\DisableDoubleQuerySdbs","NAME NOT
FOUND","Length: 20"
"23:43:40,6787304","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6787487","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Desir
Access: Read"
"23:43:40,6787700","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ,Length: 24,Data: sysmain.sdb"
"23:43:40,6787884","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ"
"23:43:40,6788079","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS",""
"23:43:40,6788254","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6788436","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6788658","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6788980","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6789147","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysmain.sdb","NAME NOT FOUND","Length:
0"
```

```
"23:43:40,6789297","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6789475","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:15,LastAccessTime: 20.11.2025 23:43:40,LastWriteTime: 20.11.2025
23:23:34,ChangeTime: 20.11.2025 23:23:34,FileAttributes: A"
"23:43:40,6790984","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6791568","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager","REPARSE","Desired Access: Query Value"
"23:43:40,6791785","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager","SUCCESS","Desired Access: Query Value"
"23:43:40,6791982","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
Manager\SafeDllSearchMode","NAME NOT FOUND","Length: 16"
"23:43:40,6793554","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Read Attributes,Disposition: Open,Options: Open Reparse Point,Attributes:
n/a,ShareMode: Read,Write,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6793810","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:15,LastAccessTime: 20.11.2025 23:43:40,LastWriteTime: 20.11.2025
23:23:34,ChangeTime: 20.11.2025 23:23:34,FileAttributes: A"
"23:43:40,6793972","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6794965","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Generic Read/Execute,Disposition: Open,Options: Synchronous IO Non-Alert,Non-
File,Attributes: n/a,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult:
Opened"
"23:43:40,6795375","parent.exe","20288","CreateFileMapping","C:\Users\kseni\lab3OSWaL
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READ|PAGE_NOCACHE"
"23:43:40,6795672","parent.exe","20288","CreateFileMapping","C:\Users\kseni\lab3OSWaL
SyncTypeOther"
"23:43:40,6796045","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6799785","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6800329","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
Folders","SUCCESS","Desired Access: Query Value"
"23:43:40,6800563","parent.exe","20288","RegQueryValue","HKCU\Software\Microsoft\Wind
Folders\Cache","SUCCESS","Type: REG_SZ,Length: 114,Data: C:\Users\kseni\AppData\Local
"23:43:40,6800766","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
Folders","SUCCESS",""
"23:43:40,6801018","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Owner,Group,DACL,SACL,Label,Attribute,Process Trust Label,0x100"
"23:43:40,6801249","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:15,LastAccessTime: 20.11.2025 23:43:40,LastWriteTime: 20.11.2025
23:23:34,ChangeTime: 20.11.2025 23:23:34,FileAttributes: A"
"23:43:40,6801976","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6802174","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysmain.sdb","NAME NOT FOUND","Length:
0"
```

```
"23:43:40,6802324","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6803262","parent.exe","20288","CreateFile","C:\Windows\apppatch\sysmain.sdb
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6803803","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6803944","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6804110","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\sysma
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READ|PAGE_NOCACHE"
"23:43:40,6804266","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6804538","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\sysma
SyncTypeOther"
"23:43:40,6805055","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6805246","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\DisableDoubleQuerySdbs","NAME NOT
FOUND","Length: 20"
"23:43:40,6805399","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6805582","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Desir
Access: Read"
"23:43:40,6805805","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ,Length: 24,Data: sysmain.sdb"
"23:43:40,6805946","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ"
"23:43:40,6806103","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS",""
"23:43:40,6806260","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6806404","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6806531","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6806677","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6806844","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
```

```
0"
"23:43:40,6806965","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6807747","parent.exe","20288","CreateFile","C:\Windows\apppatch\MergeSdbFil
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6808286","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6808529","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6808744","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\Merg
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READ|PAGE_NOCACHE"
"23:43:40,6808967","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6809396","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\Merg
SyncTypeOther"
"23:43:40,6811446","parent.exe","20288","CloseFile","C:\Windows\apppatch\sysmain.sdb"
"23:43:40,6812604","parent.exe","20288","CloseFile","C:\Windows\apppatch\MergeSdbFile
"23:43:40,6813637","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6824945","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Read Attributes,Disposition: Open,Options: Open Reparse Point,Attributes:
n/a,ShareMode: Read,Write,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6825463","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:21,LastAccessTime: 20.11.2025 23:39:09,LastWriteTime: 20.11.2025
23:23:37,ChangeTime: 20.11.2025 23:23:37,FileAttributes: A"
"23:43:40,6825757","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6828197","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Read Attributes,Disposition: Open,Options: Open Reparse Point,Attributes:
n/a,ShareMode: Read,Write,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6828612","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:21,LastAccessTime: 20.11.2025 23:39:09,LastWriteTime: 20.11.2025
23:23:37,ChangeTime: 20.11.2025 23:23:37,FileAttributes: A"
"23:43:40,6828825","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6829617","parent.exe","20288","RegOpenKey","HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\child2.exe","NAME NOT FOUND","Desired
Access: Query Value,Enumerate Sub Keys"
"23:43:40,6829915","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Wow64\x
NOT FOUND","Desired Access: Query Value"
"23:43:40,6831317","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Read Data/List Directory,Execute/Traverse,Read Attributes,Synchronize,Disposi
Open,Options: Synchronous IO Non-Alert,Non-Directory File,Attributes: N,ShareMode:
Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6832016","parent.exe","20288","CreateFileMapping","C:\Users\kseni\lab3OSWaL
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
"
"23:43:40,6832452","parent.exe","20288","CreateFileMapping","C:\Users\kseni\lab3OSWaL
SyncTypeOther"
```

```
"23:43:40,6833252","parent.exe","20288","RegOpenKey","HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\child2.exe","NAME NOT FOUND","Desired
Access: Query Value,Enumerate Sub Keys"
"23:43:40,6833844","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Label"
"23:43:40,6834716","parent.exe","20288","QueryNameInformationFile","C:\Users\kseni\la
\Users\kseni\lab3OSWaL\lab3OS\build\bin\child2.exe"
"23:43:40,6899143","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\S
Access: All Access"
"23:43:40,6899584","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 40"
"23:43:40,6900087","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
"23:43:40,6900393","parent.exe","20288","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\C
Manager\BAM","REPARSE","Desired Access: Query Value"
"23:43:40,6900753","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\C
Manager\BAM","NAME NOT FOUND","Desired Access: Query Value"
"23:43:40,6901308","parent.exe","20288","Process Create","C:\Users\kseni\lab3OSWaL\la
20140,Command line: child2.exe child1_to_child2 child2_to_parent"
"23:43:40,6902597","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
Folders","SUCCESS","Desired Access: Query Value"
"23:43:40,6902929","parent.exe","20288","RegQueryValue","HKCU\Software\Microsoft\Wind
Folders\Cache","SUCCESS","Type: REG_SZ,Length: 114,Data: C:\Users\kseni\AppData\Local
"23:43:40,6903200","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
Folders","SUCCESS",""
"23:43:40,6903438","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS","Desired Access: Query Value"
"23:43:40,6903866","parent.exe","20288","RegQueryValue","HKCU\Software\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\kseni\lab3OSWaL\lab3OS\build\bin\chi
NOT FOUND","Length: 16"
"23:43:40,6904060","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS",""
"23:43:40,6904419","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Owner,Group,DACL,SACL,Label,Attribute,Process Trust Label,0x100"
"23:43:40,6905094","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6905468","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\DisableDoubleQuerySdbs","NAME NOT
FOUND","Length: 20"
"23:43:40,6905809","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6906098","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Desir
Access: Read"
"23:43:40,6906437","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ,Length: 24,Data: sysmain.sdb"
"23:43:40,6906671","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
```

```
0,Type: REG_SZ"
"23:43:40,6906909","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS",""
"23:43:40,6907155","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6907392","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6907606","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6908086","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6908335","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysmain.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6908549","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6908833","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:21,LastAccessTime: 20.11.2025 23:39:09,LastWriteTime: 20.11.2025
23:23:37,ChangeTime: 20.11.2025 23:23:37,FileAttributes: A"
"23:43:40,6909682","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:21,LastAccessTime: 20.11.2025 23:39:09,LastWriteTime: 20.11.2025
23:23:37,ChangeTime: 20.11.2025 23:23:37,FileAttributes: A"
"23:43:40,6910009","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Owner"
"23:43:40,6910567","parent.exe","20288","QueryNameInformationFile","C:\Users\kseni\la
\Users\kseni\lab3OSWaL\lab3OS\build\bin\child2.exe"
"23:43:40,6911425","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6911664","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysmain.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6911832","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6913139","parent.exe","20288","CreateFile","C:\Windows\apppatch\sysmain.sdb
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6913852","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6914351","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6914626","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\sysm
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READWRITE"
"23:43:40,6914883","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
```

```
False"
"23:43:40,6915349","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\sysm
SyncTypeOther"
"23:43:40,6916246","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6916549","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\DisableDoubleQuerySdbs","NAME NOT
FOUND","Length: 20"
"23:43:40,6916806","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6917051","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Desir
Access: Read"
"23:43:40,6917314","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ,Length: 24,Data: sysmain.sdb"
"23:43:40,6917543","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ"
"23:43:40,6917795","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS",""
"23:43:40,6918046","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6918331","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6918592","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6918880","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6919148","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6919359","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6920498","parent.exe","20288","CreateFile","C:\Windows\apppatch\MergeSdbFil
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6921185","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6921830","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6922533","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\Merg
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READWRITE"
"23:43:40,6923105","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6923536","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\Merg
```

```
SyncTypeOther"
"23:43:40,6924014","parent.exe","20288","QueryStandardInformationFile","C:\Users\ksen
15 912 960,EndOfFile: 15 912 615,NumberOfLinks: 1,DeletePending: False,Directory:
False"
"23:43:40,6924411","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS","Desired Access: Read"
"23:43:40,6924666","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\kseni\lab3OSWaL\lab3OS\build\bin\chi
NOT FOUND","Length: 1 024"
"23:43:40,6924856","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS",""
"23:43:40,6925055","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS","Desired Access: Read"
"23:43:40,6925275","parent.exe","20288","RegQueryValue","HKCU\Software\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\kseni\lab3OSWaL\lab3OS\build\bin\chi
NOT FOUND","Length: 1 024"
"23:43:40,6925428","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS",""
"23:43:40,6925576","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Custom\child2.exe","NAME NOT FOUND","Desired
Access: Read"
"23:43:40,6930359","parent.exe","20288","QueryStandardInformationFile","C:\Users\ksen
15 912 960,EndOfFile: 15 912 615,NumberOfLinks: 1,DeletePending: False,Directory:
False"
"23:43:40,6931356","parent.exe","20288","CreateFileMapping","C:\Users\kseni\lab3OSWaL
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READ|PAGE_NOCACHE"
"23:43:40,6931628","parent.exe","20288","QueryStandardInformationFile","C:\Users\ksen
15 912 960,EndOfFile: 15 912 615,NumberOfLinks: 1,DeletePending: False,Directory:
False"
"23:43:40,6932166","parent.exe","20288","CreateFileMapping","C:\Users\kseni\lab3OSWaL
SyncTypeOther"
"23:43:40,6946364","parent.exe","20288","CloseFile","C:\Windows\apppatch\sysmain.sdb"
"23:43:40,6947004","parent.exe","20288","CloseFile","C:\Windows\apppatch\MergeSdbFile
"23:43:40,6947428","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:21,LastAccessTime: 20.11.2025 23:39:09,LastWriteTime: 20.11.2025
23:23:37,ChangeTime: 20.11.2025 23:23:37,FileAttributes: A"
"23:43:40,6947920","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
Access: Read"
"23:43:40,6948186","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NOT FOUND","Length: 20"
"23:43:40,6948370","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
"23:43:40,6956599","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
Folders","SUCCESS","Desired Access: Query Value"
"23:43:40,6956833","parent.exe","20288","RegQueryValue","HKCU\Software\Microsoft\Wind
Folders\Cache","SUCCESS","Type: REG_SZ,Length: 114,Data: C:\Users\kseni\AppData\Local
"23:43:40,6957167","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
Folders","SUCCESS",""
```

```
"23:43:40,6957358","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Owner,Group,DACL,SACL,Label,Attribute,Process Trust Label,0x100"
"23:43:40,6957754","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6957966","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\DisableDoubleQuerySdbs","NAME NOT
FOUND","Length: 20"
"23:43:40,6958143","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6958315","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Desir
Access: Read"
"23:43:40,6958514","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ,Length: 24,Data: sysmain.sdb"
"23:43:40,6958665","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ"
"23:43:40,6958830","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS",""
"23:43:40,6958945","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6959062","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6959166","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6959389","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6959496","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysmain.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6959593","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6959711","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:21,LastAccessTime: 20.11.2025 23:43:40,LastWriteTime: 20.11.2025
23:23:37,ChangeTime: 20.11.2025 23:23:37,FileAttributes: A"
"23:43:40,6960682","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6962319","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
Access: Read Attributes,Disposition: Open,Options: Open Reparse Point,Attributes:
n/a,ShareMode: Read,Write,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6962604","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:21,LastAccessTime: 20.11.2025 23:43:40,LastWriteTime: 20.11.2025
23:23:37,ChangeTime: 20.11.2025 23:23:37,FileAttributes: A"
"23:43:40,6962747","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6963647","parent.exe","20288","CreateFile","C:\Users\kseni\lab3OSWaL\lab3OS
```

```
Access: Generic Read/Execute,Disposition: Open,Options: Synchronous IO Non-Alert,Non-
File,Attributes: n/a,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult:
Opened"
"23:43:40,6963960","parent.exe","20288","CreateFileMapping","C:\Users\kseni\lab3OSWaL
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READ|PAGE_NOCACHE"
"23:43:40,6964152","parent.exe","20288","CreateFileMapping","C:\Users\kseni\lab3OSWaL
SyncTypeOther"
"23:43:40,6964389","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6966930","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:43:40,6967273","parent.exe","20288","RegOpenKey","HKCU\Software\Microsoft\Windows
Folders","SUCCESS","Desired Access: Query Value"
"23:43:40,6967452","parent.exe","20288","RegQueryValue","HKCU\Software\Microsoft\Wind
Folders\Cache","SUCCESS","Type: REG_SZ,Length: 114,Data: C:\Users\kseni\AppData\Local
"23:43:40,6967610","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
Folders","SUCCESS",""
"23:43:40,6967786","parent.exe","20288","QuerySecurityFile","C:\Users\kseni\lab3OSWaL
Owner,Group,DACL,SACL,Label,Attribute,Process Trust Label,0x100"
"23:43:40,6967917","parent.exe","20288","QueryBasicInformationFile","C:\Users\kseni\l
20.11.2025 23:18:21,LastAccessTime: 20.11.2025 23:43:40,LastWriteTime: 20.11.2025
23:23:37,ChangeTime: 20.11.2025 23:23:37,FileAttributes: A"
"23:43:40,6968275","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6968401","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysmain.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6968505","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6969160","parent.exe","20288","CreateFile","C:\Windows\apppatch\sysmain.sdb
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6969520","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6969615","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6969727","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\sysm
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READ|PAGE_NOCACHE"
"23:43:40,6969837","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
4 128 768,EndOfFile: 4 127 356,NumberOfLinks: 3,DeletePending: False,Directory:
False"
"23:43:40,6970014","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\sysm
SyncTypeOther"
"23:43:40,6970339","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6970502","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
```

```
NT\CurrentVersion\AppCompatFlags\SdbUpdates\DisableDoubleQuerySdbs","NAME NOT
FOUND","Length: 20"
"23:43:40,6970634","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6970783","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Desir
Access: Read"
"23:43:40,6970975","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ,Length: 24,Data: sysmain.sdb"
"23:43:40,6971112","parent.exe","20288","RegEnumValue","HKLM\SOFTWARE\Microsoft\Windo
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS","Index
0,Type: REG_SZ"
"23:43:40,6971252","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates\ManifestedMergeStubSdbs","SUCCESS",""
"23:43:40,6971401","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6971553","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6971665","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6971864","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS","Desired Access: Read"
"23:43:40,6972024","parent.exe","20288","RegQueryValue","HKLM\SOFTWARE\Microsoft\Wind
NT\CurrentVersion\AppCompatFlags\SdbUpdates\sysMerge.sdb","NAME NOT FOUND","Length:
0"
"23:43:40,6972184","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\AppCompatFlags\SdbUpdates","SUCCESS",""
"23:43:40,6972748","parent.exe","20288","CreateFile","C:\Windows\apppatch\MergeSdbFil
Access: Generic Read,Disposition: Open,Options: Synchronous IO Non-Alert,Non-Director
File,Attributes: N,ShareMode: Read,Delete,AllocationSize: n/a,OpenResult: Opened"
"23:43:40,6973194","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6973288","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6973423","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\Merg
LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection,PageProtection:
PAGE_EXECUTE_READ|PAGE_NOCACHE"
"23:43:40,6973561","parent.exe","20288","QueryStandardInformationFile","C:\Windows\ap
32 768,EndOfFile: 31 900,NumberOfLinks: 2,DeletePending: False,Directory: False"
"23:43:40,6973798","parent.exe","20288","CreateFileMapping","C:\Windows\apppatch\Merg
SyncTypeOther"
"23:43:40,6975390","parent.exe","20288","CloseFile","C:\Windows\apppatch\sysmain.sdb"
"23:43:40,6976250","parent.exe","20288","CloseFile","C:\Windows\apppatch\MergeSdbFile
"23:43:40,6976946","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:44:10,6672035","parent.exe","20288","Thread Exit","","SUCCESS","Thread
ID: 20352,User Time: 0.0000000,Kernel Time: 0.0000000"
```

```
"23:44:10,6672537","parent.exe","20288","Thread Exit","","SUCCESS","Thread
ID: 19752,User Time: 0.0000000,Kernel Time: 0.0000000"
"23:44:24,5384975","parent.exe","20288","QueryNameInformationFile","C:\Users\kseni\la
\Users\kseni\lab3OSWaL\lab3OS\build\bin\child1.exe"
"23:44:24,5385622","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\child1.exe","NAME NOT FOUND","Desired
Access: Query Value"
"23:44:24,5463634","parent.exe","20288","QueryNameInformationFile","C:\Users\kseni\la
\Users\kseni\lab3OSWaL\lab3OS\build\bin\child2.exe"
"23:44:24,5464211","parent.exe","20288","RegOpenKey","HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\child2.exe","NAME NOT FOUND","Desired
Access: Query Value"
"23:44:24,5527866","parent.exe","20288","Thread Exit","","SUCCESS","Thread
ID: 20272,User Time: 0.0000000,Kernel Time: 0.0000000"
"23:44:24,5532847","parent.exe","20288","Process Exit","","SUCCESS","Exit Status:
0,User Time: 0.0000000 seconds,Kernel Time: 0.0000000 seconds,Private Bytes:
790 528,Peak Private Bytes: 880 640,Working Set: 18 178 048,Peak Working Set:
18 178 048"
"23:44:24,5533397","parent.exe","20288","RegOpenKey","HKLM\System\CurrentControlSet\S
Access: All Access"
"23:44:24,5533803","parent.exe","20288","RegQueryValue","HKLM\System\CurrentControlSe
NOT FOUND","Length: 40"
"23:44:24,5534207","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
"23:44:24,5535345","parent.exe","20288","CloseFile","C:\Users\kseni\lab3OSWaL\lab3OS\
"23:44:24,5536566","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
"23:44:24,5536996","parent.exe","20288","RegCloseKey","HKLM\SOFTWARE\Microsoft\Window
NT\CurrentVersion\Image File Execution Options","SUCCESS",""
"23:44:24,5537277","parent.exe","20288","RegCloseKey","HKCU\Software\Microsoft\Window
NT\CurrentVersion","SUCCESS",""
"23:44:24,5537421","parent.exe","20288","RegCloseKey","HKLM\System\CurrentControlSet\
Manager","SUCCESS",""
```