ІПЗ-33\1 Гоша Давід Олександрович

Лабораторна №3

Назва програми	Призначення	Об’єкт дослідження	Результати дослідження	Оцінка	Висновки (позитвні і негативні)
RegMon	Стежить за зверненням програм, що запускаються або вже працюють, до диска або системного реєстру комп'ютера.	Internet Explorer (IE)	Режим перехоплення звернень до реєстру краще безпосередньо перед виконанням зміни домашньої сторінки IE, щоб зменшити обсяг аналізованої інформації, що не стосується проблеми, що шукається.	3	Позитивні: зручний інтерфейс, наявність фільтрів. Недоліки: Більше не підтримужться.
DiskMon	Програма, яка реєструє та відображає всі дії жорсткого диска у системі Windows.	Internet Explorer (IE)	DiskMon використовує трасування подій ядра. Трасування подій задокументовано в пакеті SDK платформи Майкрософт, а пакет SDK містить вихідний код traceDmp, на якому базується DiskMon.	4	Позитивні: збереження вмісту подання списку в файлі ASCII. Зміщення читання та запису представлені з погляду секторів (512 байт) Недоліки: DiskMon блиматиме під час кожної нової операції з диском
FileMon	Спостереження в реальному масштабі часу за діями з файлами, мережею та іменованими каналами	Internet Explorer (IE)	Після збереження налаштувань перемикаєтесь у вікно Filemon, зупиняєте процес перехоплення подій та аналізуєте отримані дані. Звичайно, у разі складної програми, операцій введення/виводу може бути	5	Позитивні: Швидкість роботі, вага программи

			чимала кількість, і доведеться розбиратися виходячи зі здорового глузду та логіки роботи програми. Так, найімовірніше, що налаштування не зберігаються у тимчасових файлах, тому їх можна відразу виключити з аналізу. Наступне припущення - налаштування браузера пов'язані з профілем користувача, отже в ньому ж повинні зберігатися. (каталог C:\documents And Settings\користувач : для Win2k/XP). Збереження настоянок – це операція запису. В результаті таких припущень коло пошуку буде значно звужено і файл налаштувань буде знайдено легко.		Недоліки: Більше не підтримужться.
PortMon	Службова програма, яка відстежує та відображає всі дії послідовного та паралельного портів у системі	Internet Explorer (IE)	PortMon VxD використовує стандартний перехоплювач служби VxD для перехоплення всіх доступу до функцій VCOMM. Як і драйвер пристрою NT, VxD Portmon інтерпретує запити для їх відображення у зрозумілому форматі. У Windows 95 і 98 Portmon відстежує всі порти, щоб не було вибору портів, як у NT.	4	Позитивні: віддалений моніторинг, Копіювання буфера обміну Недоліки: Однофайлові корисні дані
APIMon	Об'єднання відразу двох утиліт: FileMon (моніторинг файлової системи) та RegMon (моніторинг реєстру), надає користувачам потужний інструмент для моніторингу	Internet Explorer (IE)		3	Позитивні: Додаткові дані, захоплені для вхідних та вихідних параметрів операції. Фільтри, що не руйнують, дозволяють встановлювати фільтри без втрати даних.

	файлової системи, системного реєстру, а також всіх процесів в оперативній пам'яті в реальному часі.				Недоліки: Запис стеків потоків кожної операції дозволяє у багатьох випадках визначити першопричину операції.

Висновки

Вміння поводитися з реєстром є величезним плюсом для користувача будь-якого рівня. У такому разі, не чекаючи допомоги з боку, ви зможете самостійно покращити або відновити працездатність своєї операційної системи у разі серйозних проблем. Щоправда, ще важливіше не доводити свою робочу операційну систему до плачевного стану, здійснюючи моніторинг реєстру або як мінімум його постійне очищення від «сміття».

Взагалі більшість проблем з Windows, які виникають через неполадки в реєстрі, можна вирішити самостійно за допомогою порад фахівців, які прихильно розміщують в мережі інтернет. Правда, щоб скористатися ними, вам у будь-якому випадку необхідно хоча б загалом, знати, що є реєстром, і яким способом вносити до нього зміни. Ну а якщо самостійно не вдалося впоратися з виниклими неполадками, ваші базові знання допоможуть коректно пояснити суть проблеми фахівцю комп'ютерної служби, що істотно прискорить процес її усунення.