Системне програмування

Лекція № 6

Лектор Артамонов Є.Б.

Поняття процесу

- Процес – це абстрактне поняття, що описує роботу програми. Все інше базується на цьому понятті, тому представляється вкрай важливим, щоб розробники операційних систем одержали повне подання про концепції процесу якомога раніше.

Створення процесу

- 1) ініціалізація системи;
- 2) виконання виданого працюючим процесом системного запиту на створення процесу;
- 3) запит користувача на створення процесу;
- 4) ініціювання пакетного завдання.

Створення процесу

- Основні функції: CreateProcess, CreateProcessAsUser (для Win NT/2000) і CreateProcessWithLogonW (починаючи з Win2000).
- Етапи:
  - відкривається файл образу (EXE).
  - якщо виконуваний файл не являється Win32 додатком, то шукається образ підтримки (support image) для запуску цієї програми.

Етапи запуску win32 процесу

- Створюється об'єкт Win32 "процес".
- Створюється первинний потік (стек, контекст і об'єкт "потік").
- Підсистема Win32 повідомляється про створення нового процесу і потоку.
- Починається виконання первинного потоку.
- У контексті нового процесу і потоку ініціалізувався адресний простір (наприклад, завантажуються необхідні DLL) і починається виконання програми.

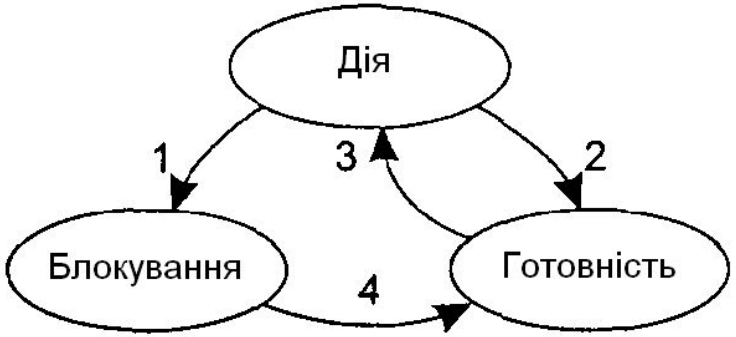
Завершення процесу

- звичайний вихід (навмисно);
- вихід помилково (навмисно);
- вихід по непоправній помилці (ненавмисно);
- знищення іншим процесом (ненавмисно).

Стани процесів

- працюючий (у цей конкретний момент використовує процесор);
- готовий до роботи (процес тимчасово припинений, щоб дозволити виконуватися іншому процесу);
- заблокований (процес не може бути запущений перш, ніж відбудеться якась зовнішня подія).

Стани процесів



1. Процес блокується, очікуючи нових даних
2. Планувальник вибирає інший процес
3. Планувальник вибврає цей процес
4. Доступні вхідні данні

Деякі поля типового елемента таблиці процесів

Керування процесом	Керування пам’яттю	Керування файлами
Регістри	Вказівник на текстовий сегмент	Корінний каталог
Лічильник команд	Вказівник на сегмент даних	Робочий каталог
Слово стану програми	Вказівник на сегмент стека	Дескриптори файлу
Вказівник стека		Ідентифікатор користувача
Стан процесу		Ідентифікатор групи
Пріоритет		
Параметри планування		
Ідентифікатор процесу		

Пріоритети процесів

- У Windows існує 32 рівні пріоритету, від 0 до 31. Вони поділяються на два блоки від 31 – 16 – пріоритети реального часу; від 15 - 1 динамічні рівні; 0 - системний пріоритет, зарезервований для потоку обнулення сторінок (zero-page thread).
- При створенні процесу, йому призначається один з шести класів пріоритетів:
  - Real time class (значення 24);
  - High class (значення 13);
  - Above normal class (значення 10),
  - Normal class (значення 8),
  - Below normal class (значення 6),
  - Idle class (значення 4).

Пріоритети потоків

- Пріоритет кожного потоку (базовий пріоритет потоку) складається з пріоритету його процесу і відносного пріоритету самого потоку.
- Є сім відносних пріоритетів потоків:
  - Normal: такий же як і у процесу;
  - Normal: +1 до пріоритету процесу;
  - Below normal: -1;
  - Highest: +2;
  - Lowest: -2;
  - Time critical: встановлює базовий пріоритет потоку для Real time класу в 31, для решти класів в 15.
  - Idle: встановлює базовий пріоритет потоку для Real time класу в 16, для решти класів в 1.

Інтерактивні та фонові процеси

- *Інтерактивні процеси* взаємодіють із користувачами безпосередньо, приймаючи від них дані, введені за допомогою клавіатури, миші тощо. Прикладом інтерактивного процесу може бути процес текстового редактора або інтегрованого середовища розробки.

- *Фонові процеси* із користувачем не взаємодіють безпосередньо. Зазвичай вонизапускаються під час старту системи і чекають на запити від інших застосувань. Деякі з них (системні процеси) підтримують функціонування системи (реалізують фонове друкування, мережні засоби тощо), інші виконують спеціалізовані задачі (реалізують веб-сервери, сервери баз даних тощо). Фонові процеси також називають службами (services, у системах лінії Windows XP) або демонами (daemons, в UNIX).

Структури даних процесу

- У режимі користувача доступним є *блок оточення процесу* (process environment block, PEB), що перебуває в адресному просторі цього процесу.

  EPROCESS і KPROCESS, на відміну від PEB, доступні тільки із привілейованого режиму.

Структури даних процесу

- Керуючий блок процесу містить такі основні елементи:
  - блок процесу ядра (KPROCESS);
  - ідентифікаційну інформацію;
  - інформацію про адресний простір процесу;
  - інформацію про ресурси, доступні процесу, та обмеження на використання цих ресурсів;
  - блок оточення процесу (PEB);
  - інформацію для підсистеми безпеки.

Ідентифікація інформації

- ідентифікатор процесу (pid);
- ідентифікатор процесу, що створив цей процес (незважаючи на те, що Windows XP не підтримує відносини «предок-нащадок» автоматично, вони можуть бути задані програмним шляхом, тобто нащадок може сам призначити собі предка, задавши цей ідентифікатор);
- ім'я завантаженого програмного файла.

Блок процесу ядра

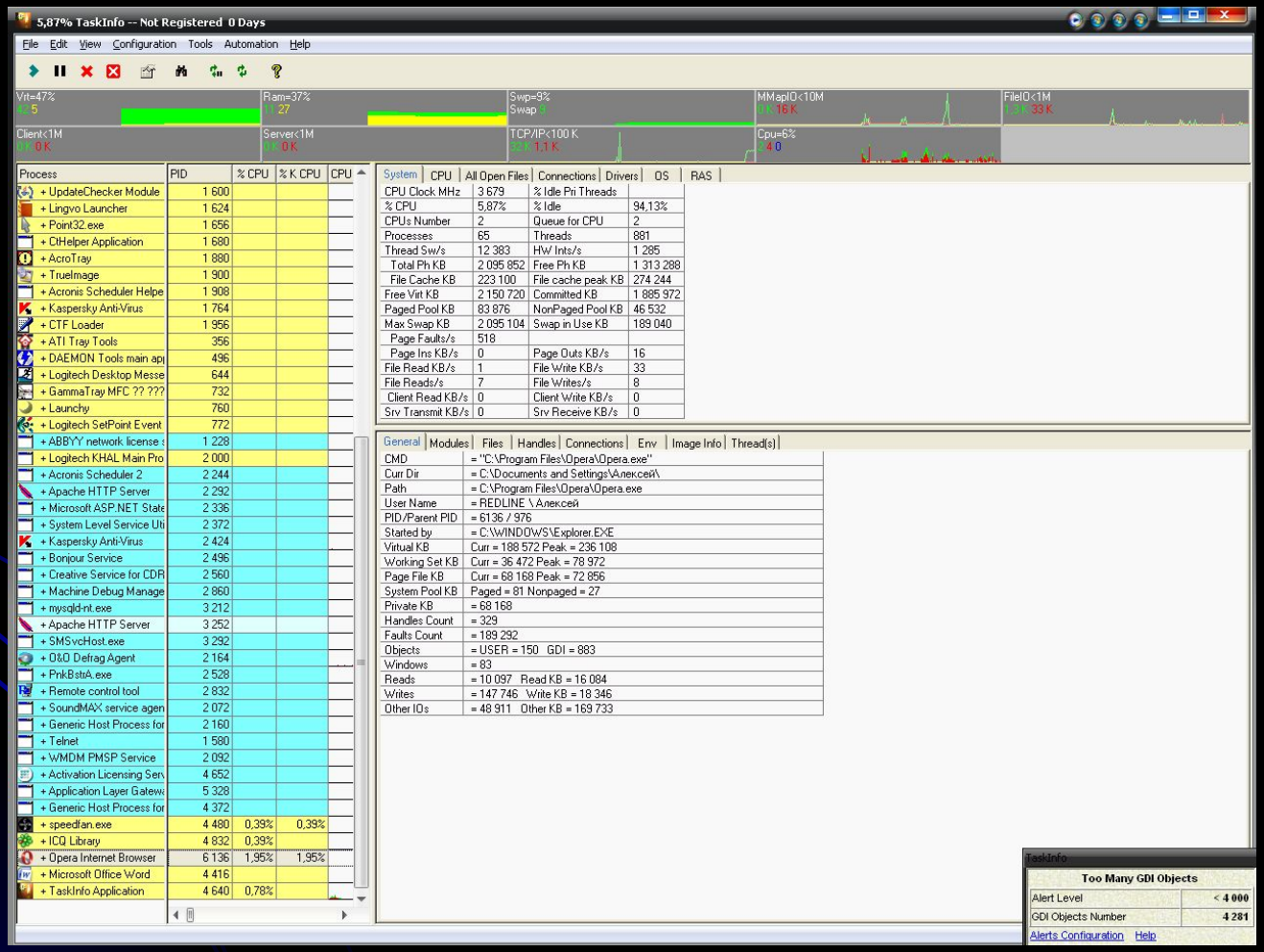
- містить усю інформацію, що належить до потоків цього процесу:
  - покажчик на ланцюжок блоків потоків ядра, де кожний блок відповідає потоку;
  - базову інформацію, необхідну ядру системи для планування потоків (ця інформація буде успадкована потоками, пов'язаними із цим процесом).

Блок оточення процесу

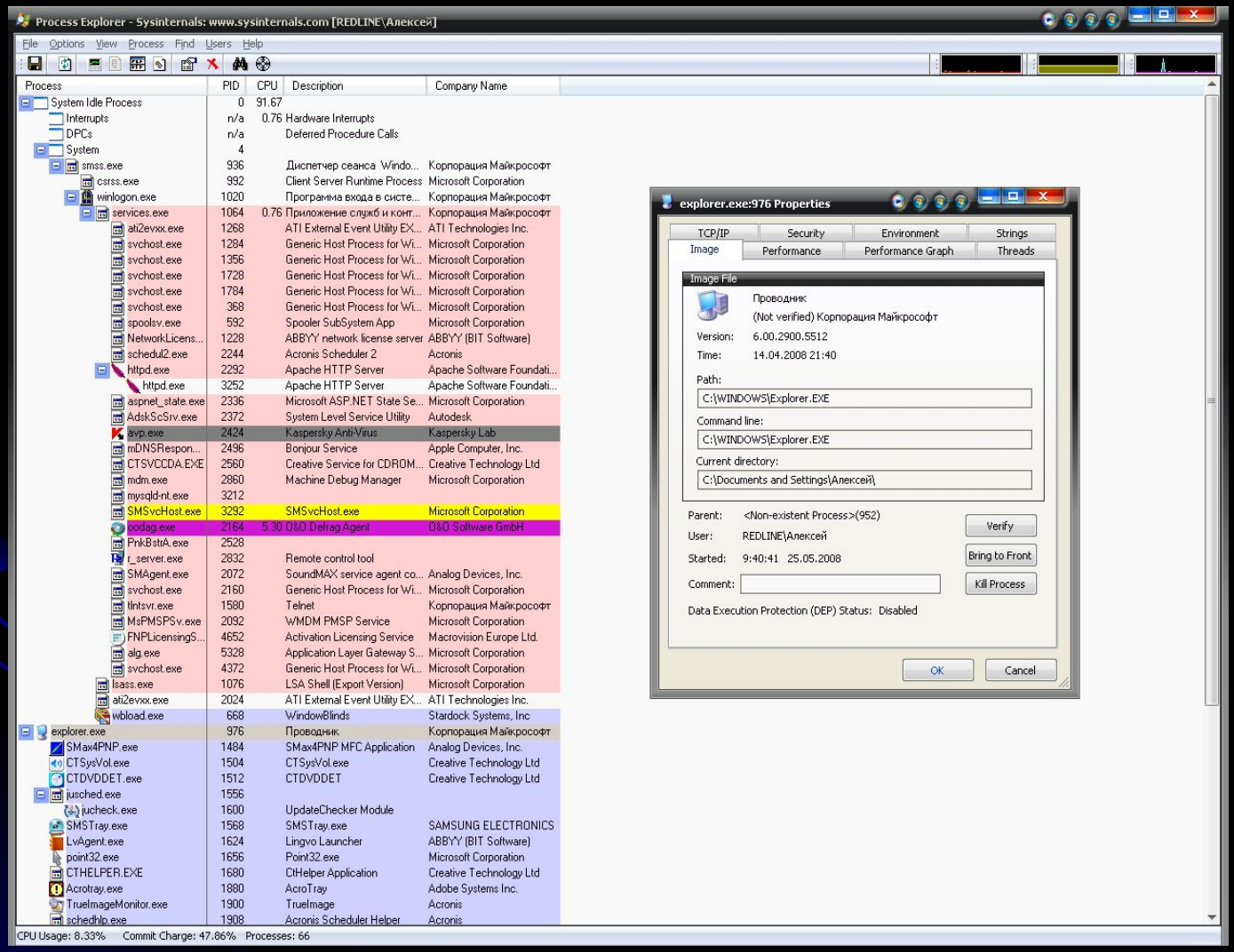
- містить інформацію про процес, яка призначена для доступу з режиму користувача:
  - початкову адресу ділянки пам'яті, куди завантажився програмний файл;
  - покажчик на динамічну ділянку пам'яті, доступну процесу.

Методи маскування і виявлення процесів в операційній системі Windows

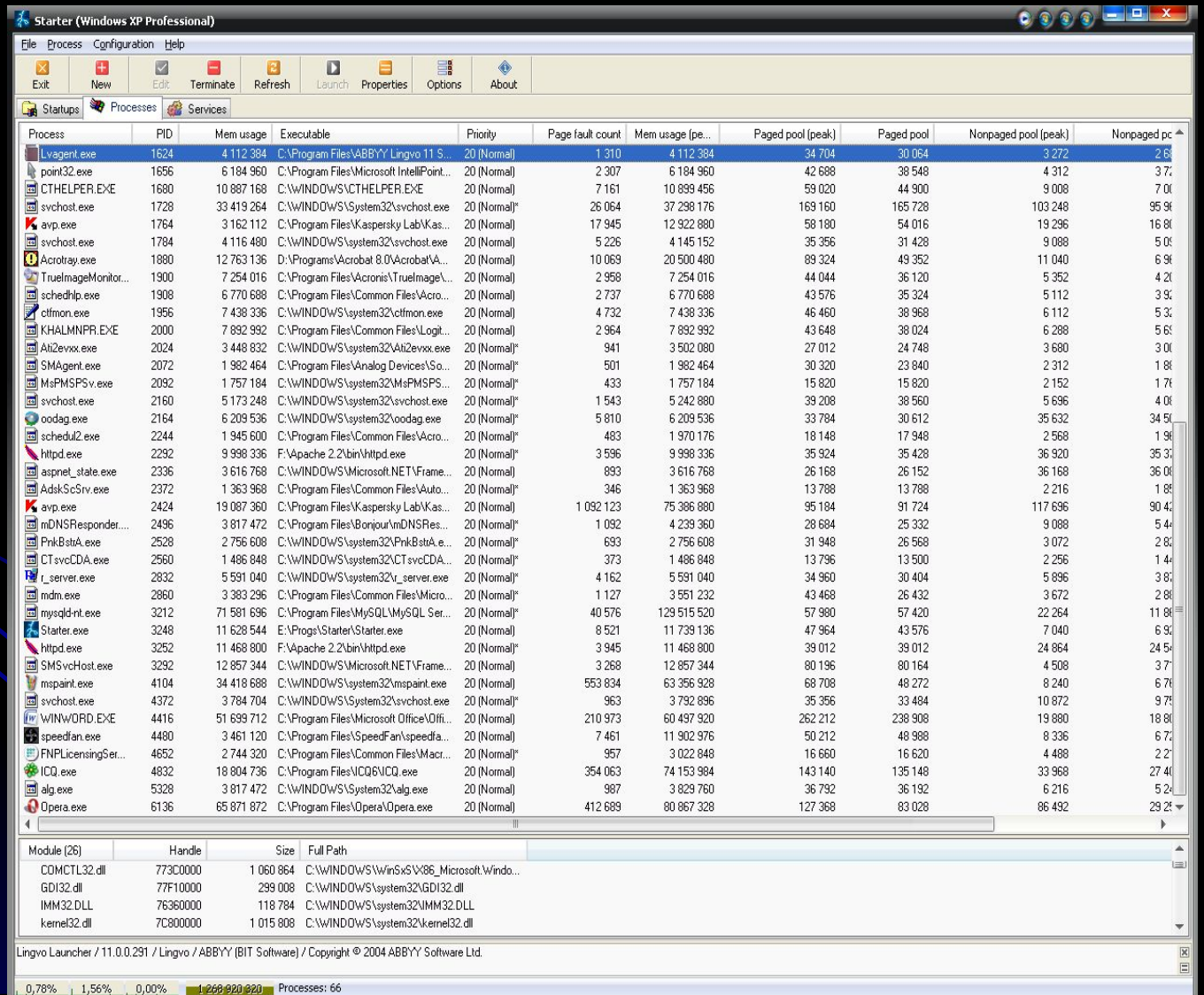
Програмне забезпечення TaskInfo



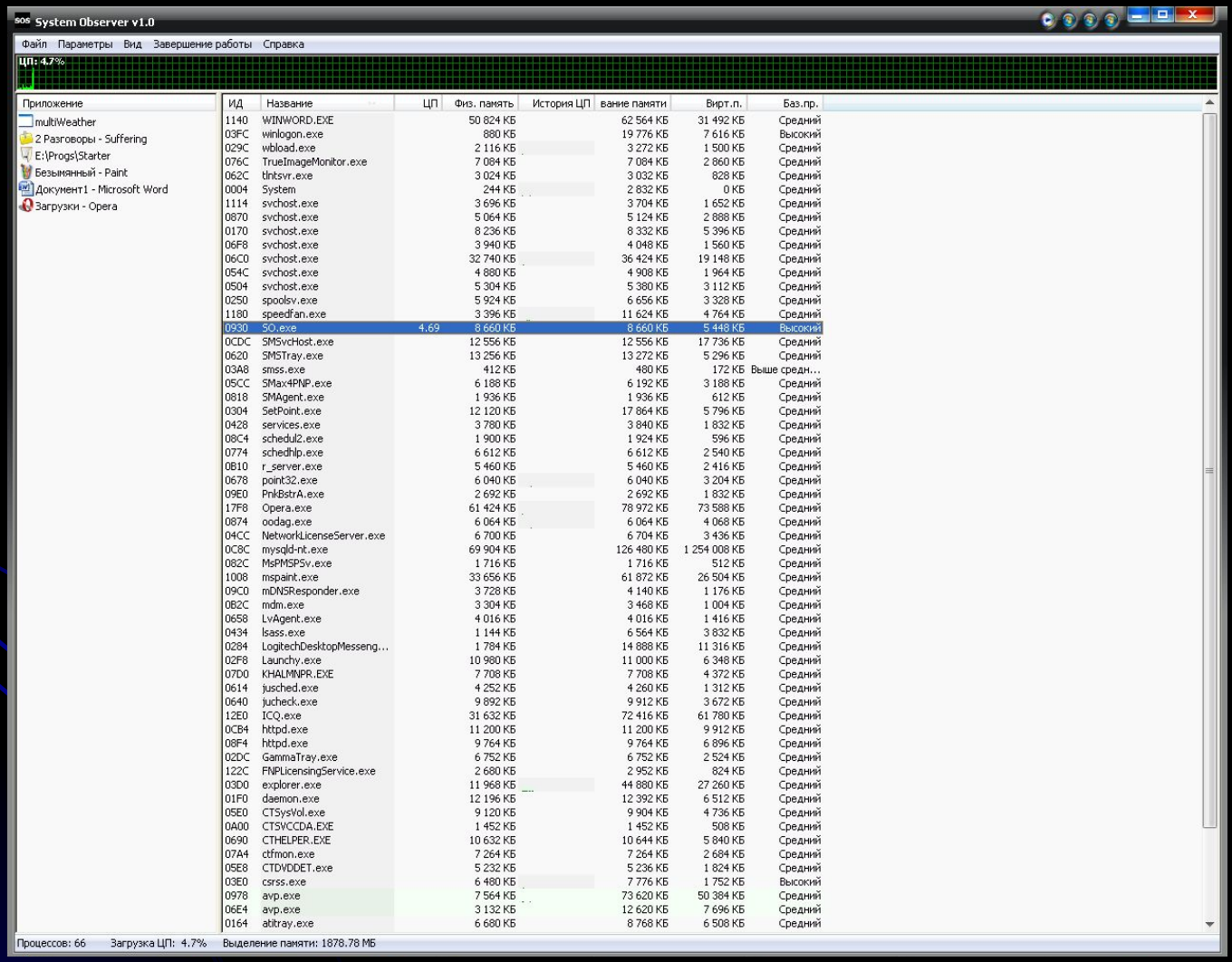
Програмне забезпечення Process Explorer



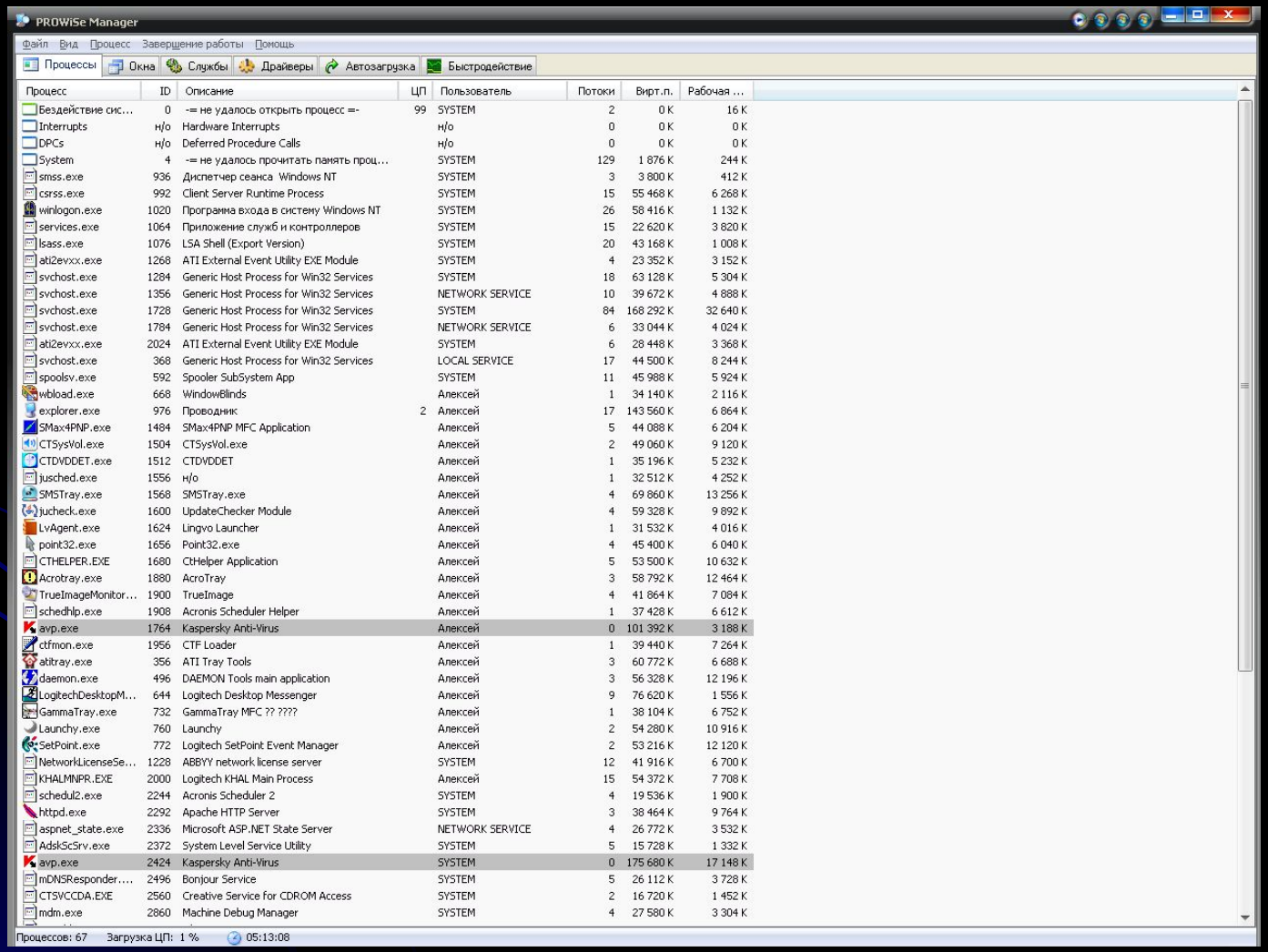
Програмне забезпечення Codestuff Starter



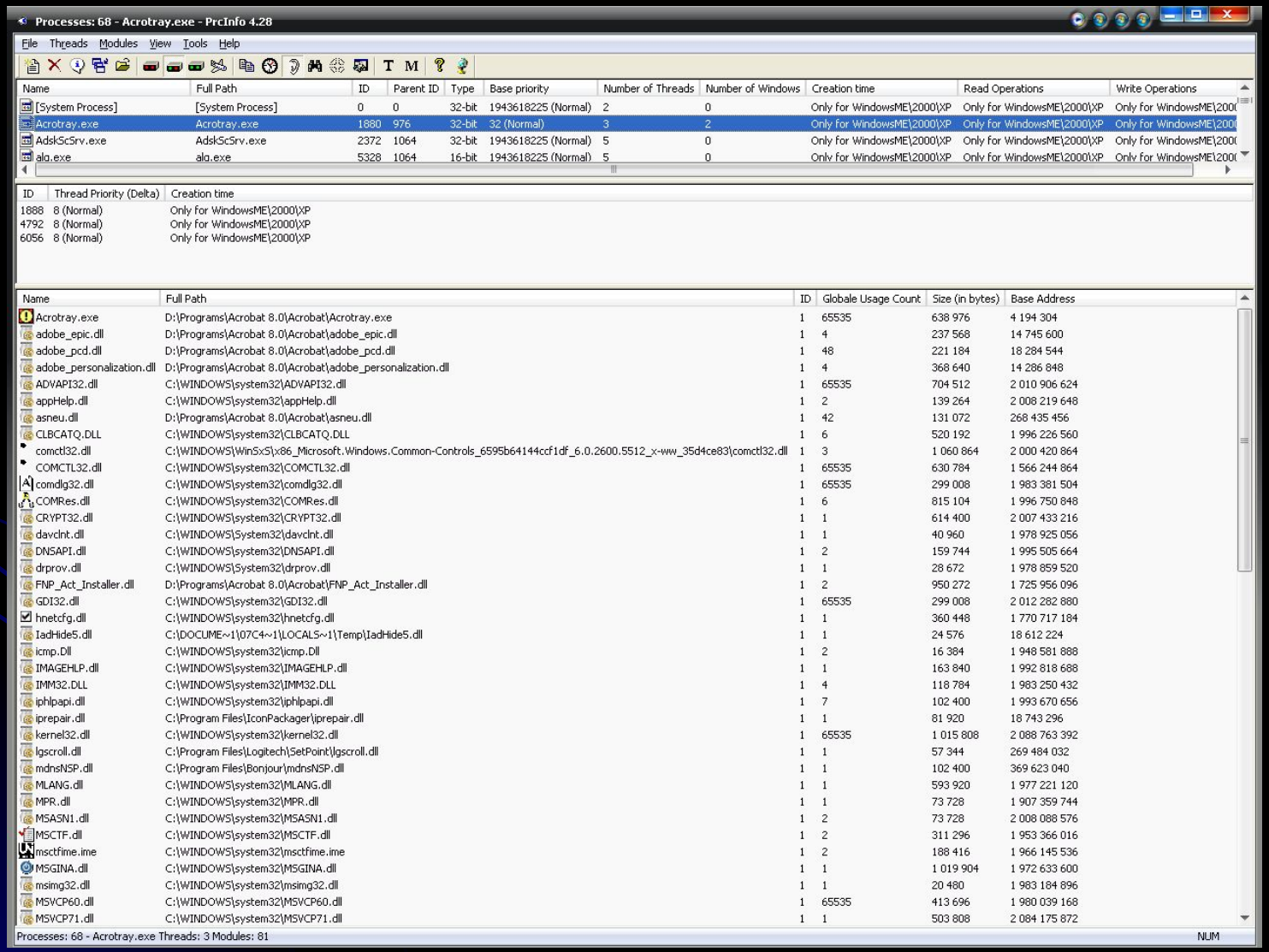
Програмне забезпечення System Observer



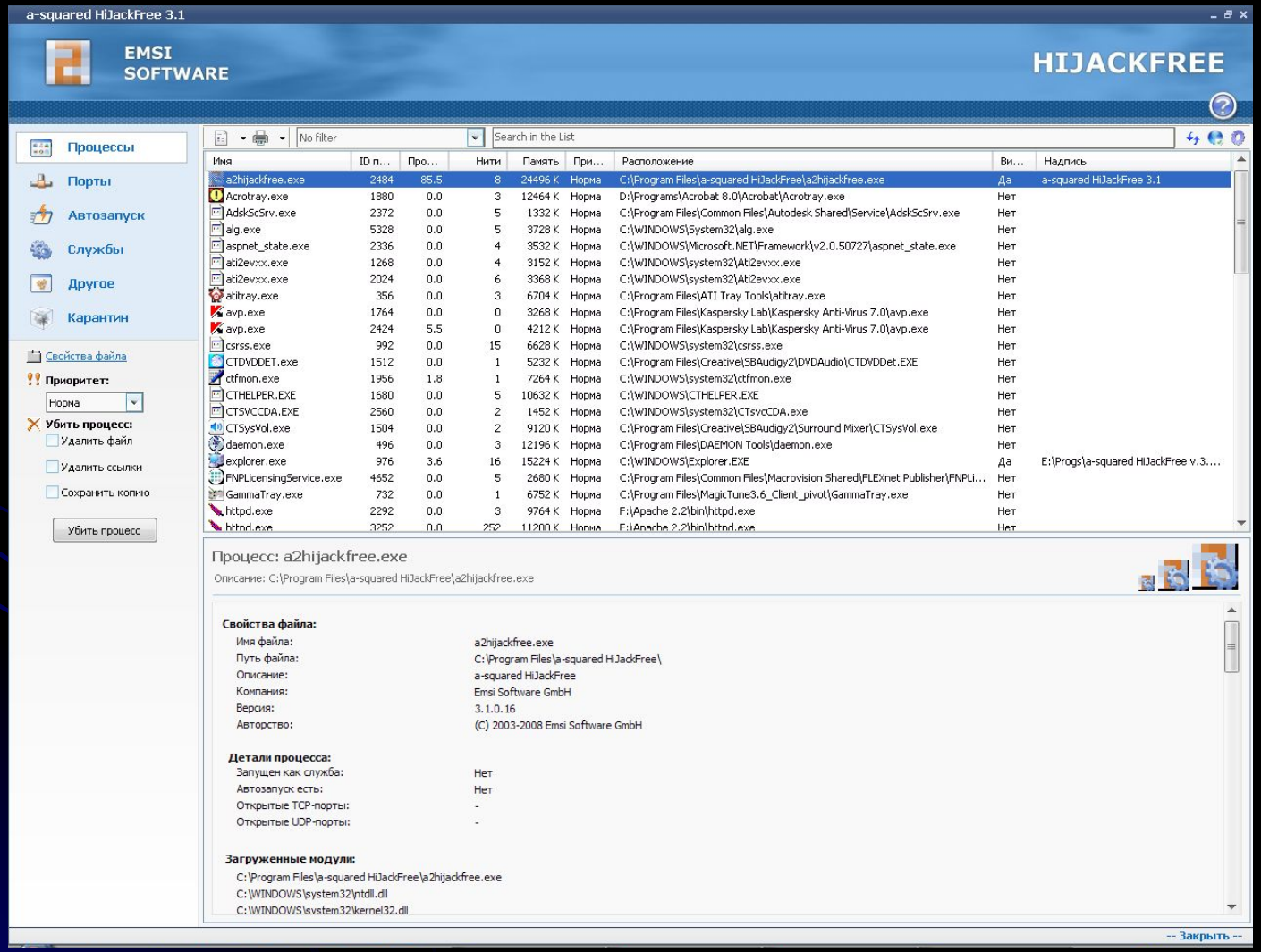
Програмне забезпечення PROWiSe Manager



Програмне забезпечення PrcInfo



Програмне забезпечення A-squared HiJackFree



Основні методи відображення прихованих процесів

Схема алгоритму отримання списку процесів через ToolHelp API

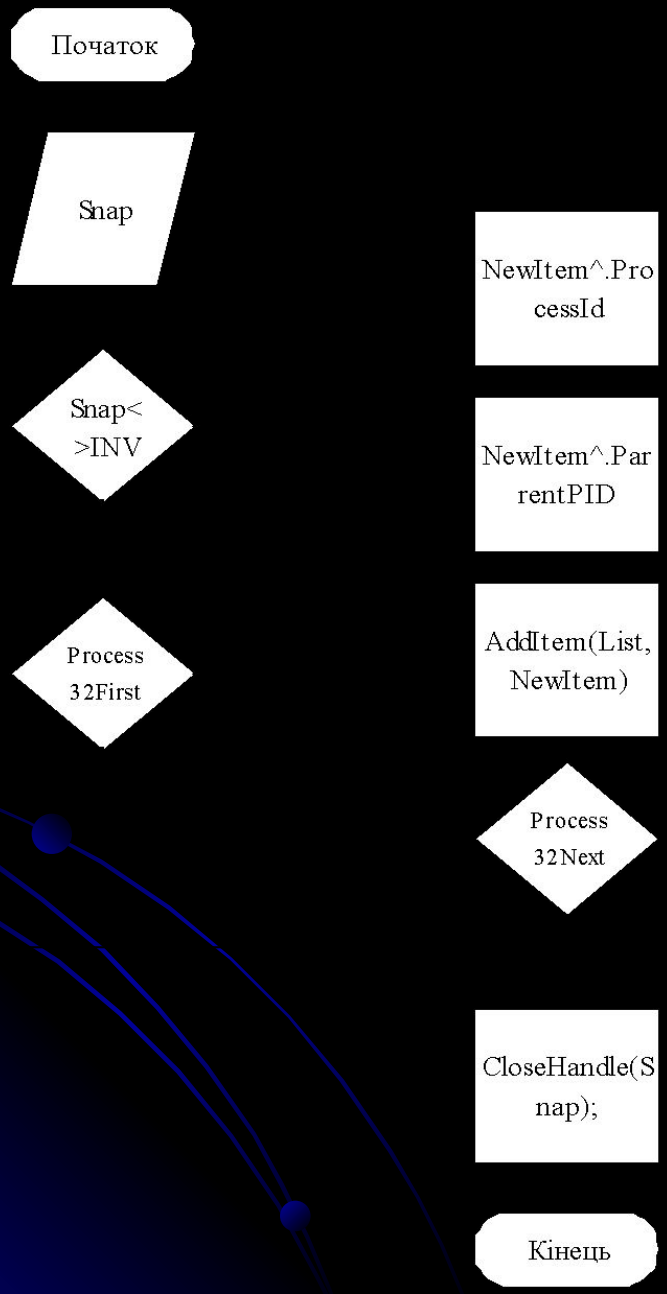
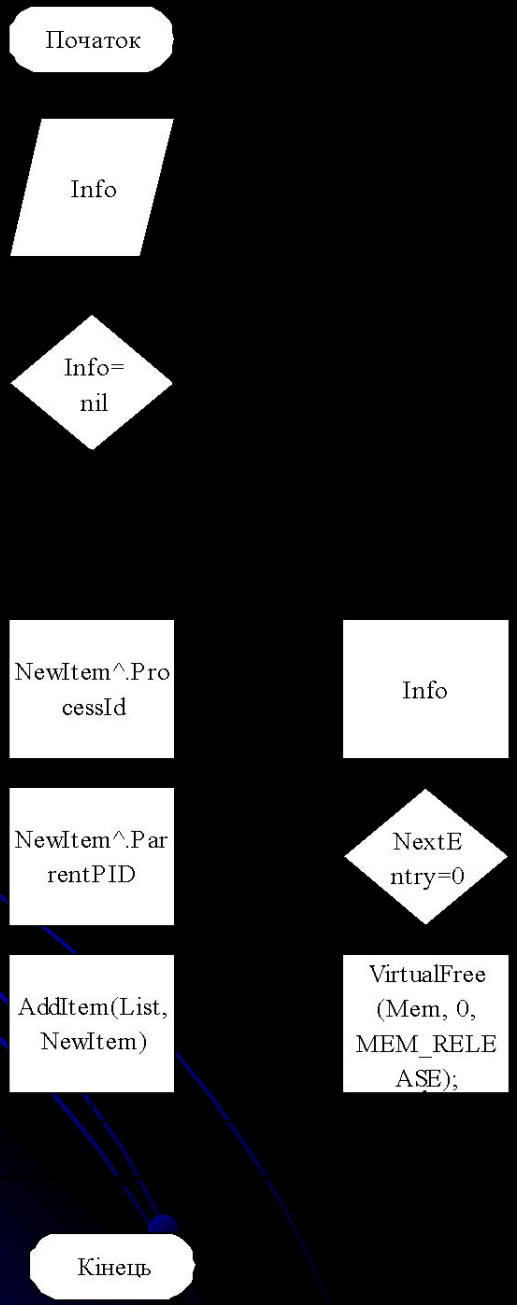
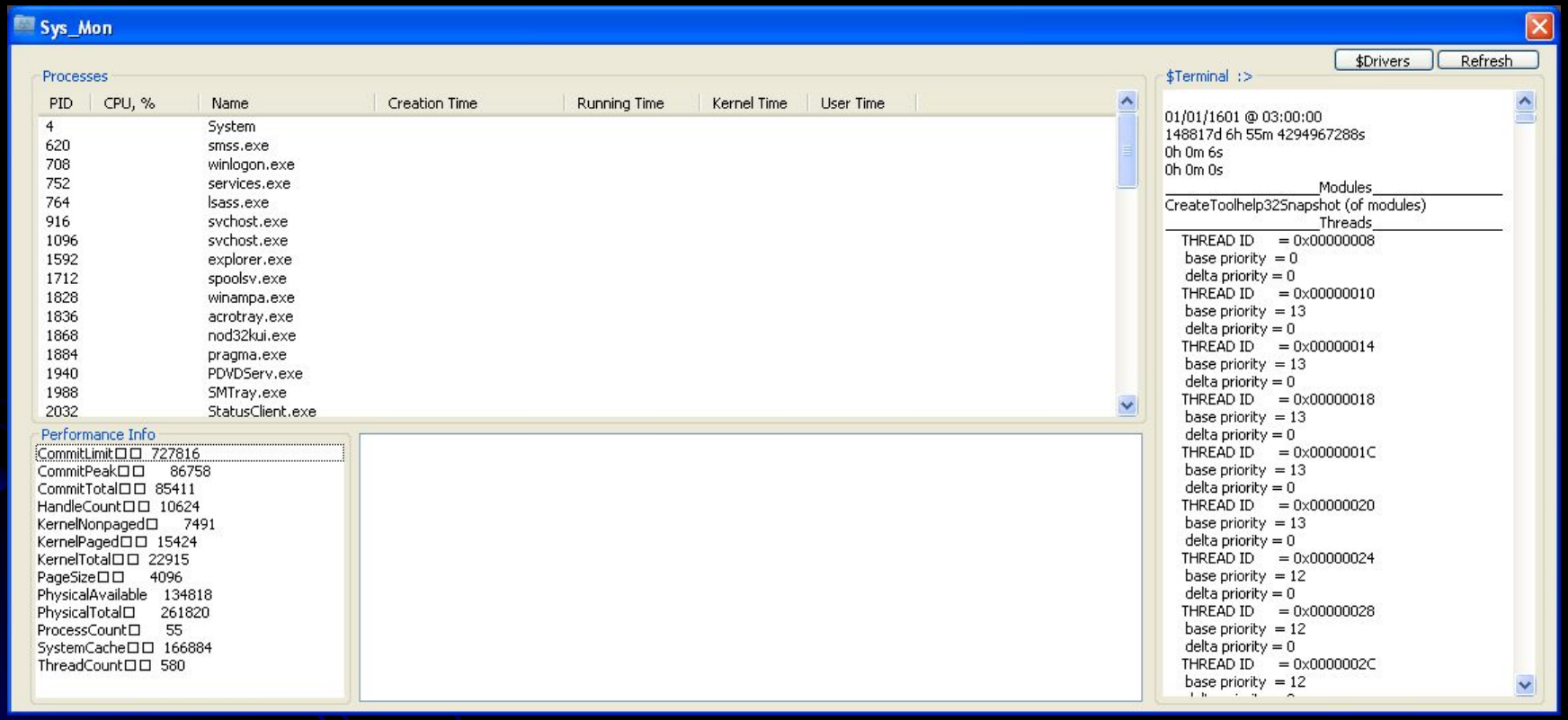


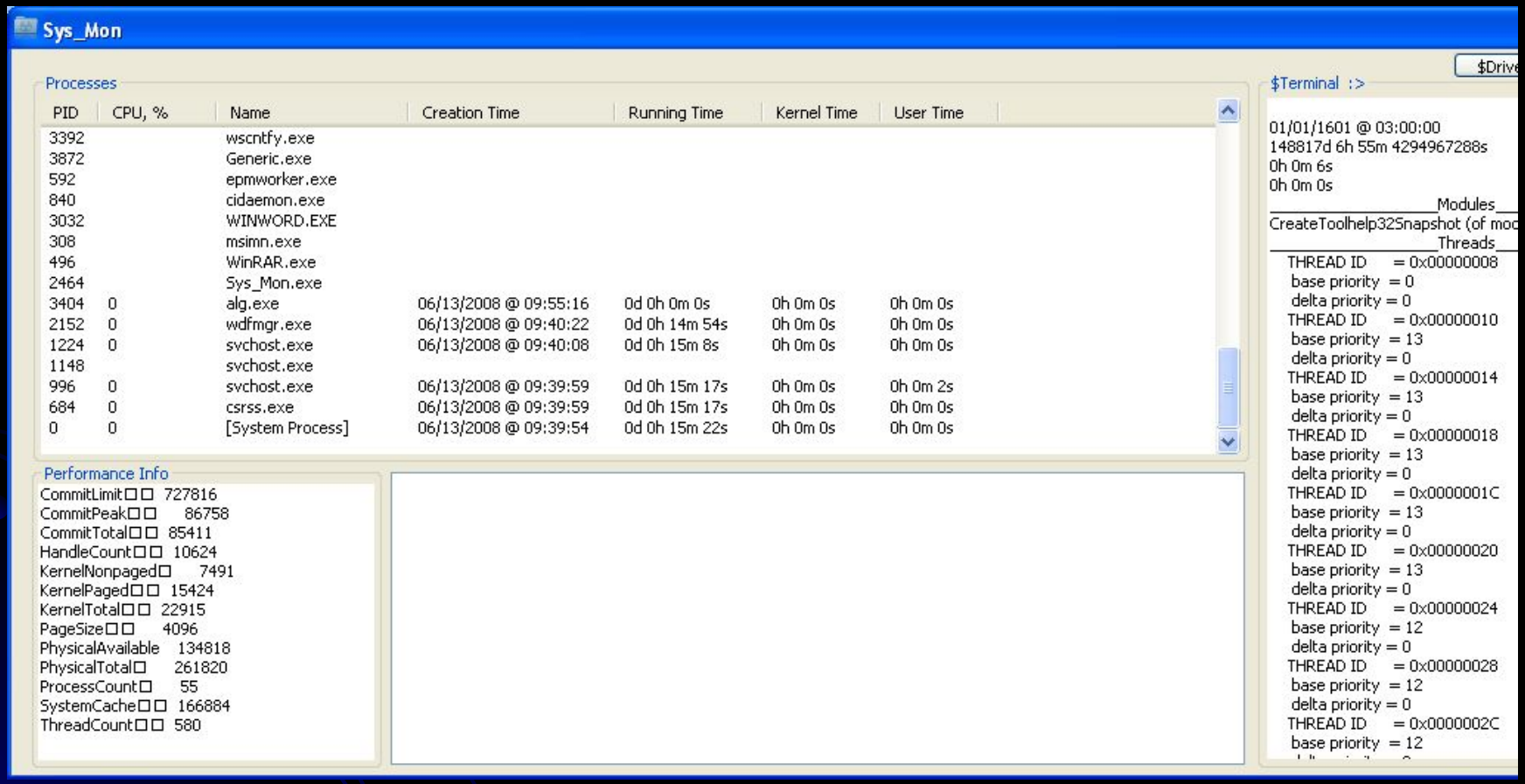
Схема алгоритму отримання списку процесів через Native API



Вид головного вікна у полегшеному режимі сканування



Вид головного вікна у поглибленому режимі сканування



Дякую за увагу!!!
Зустрінемось на лекції через тиждень

Знайти лектора можна в аудиторії 5-214
або
за e-mail-ом: eart@ukr.net
або
вКонтакте: http://vk.com/id6416748