雲端軟體分析器

以模擬器建構線上系統程式分析環境

專題生：謝居安

指導教授：謝續平

惡意程式分析現況

- 工具為數眾多且各有特點,環境建置不易
- 分析工具易被惡意程式識別

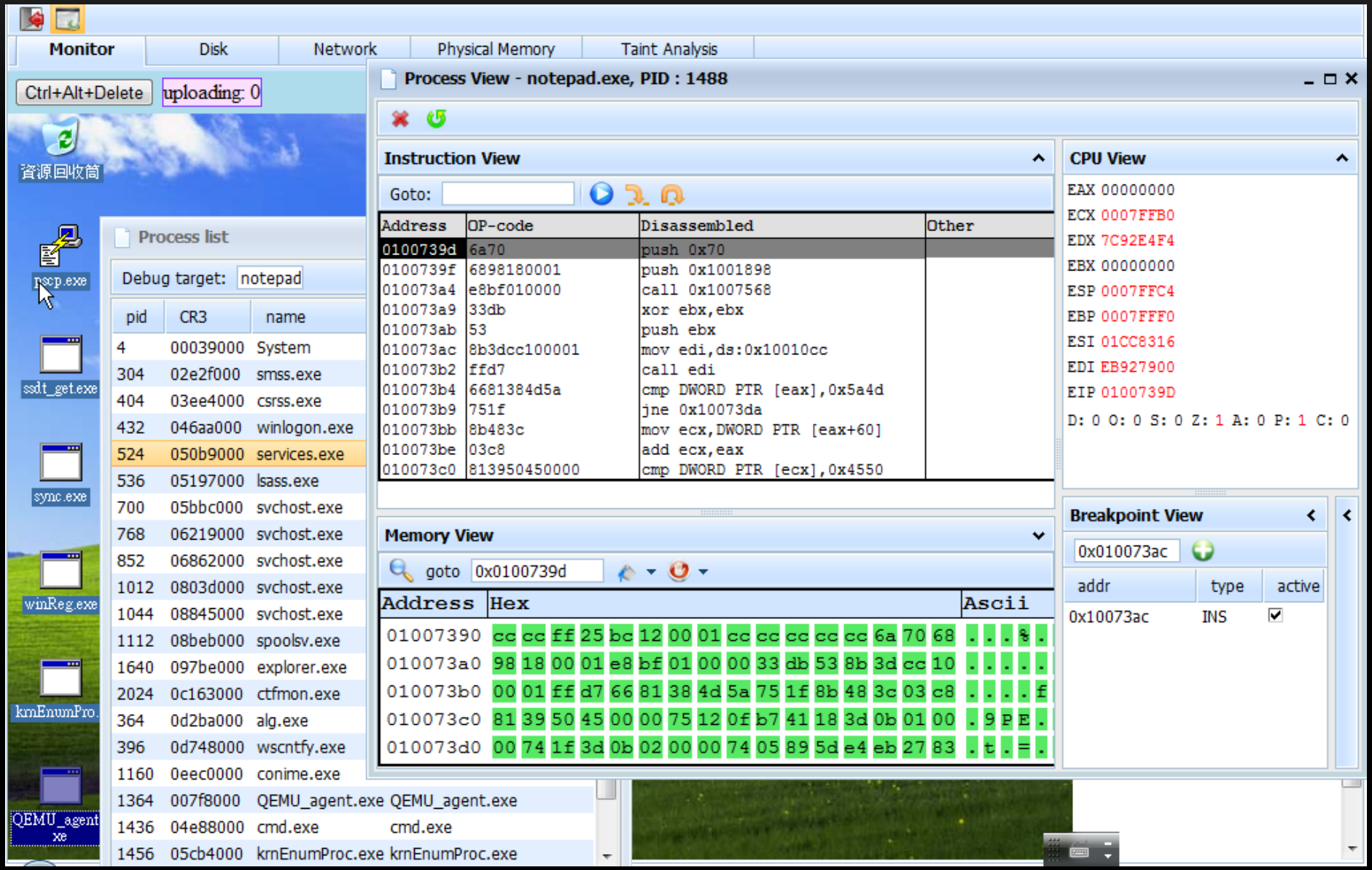
與現有線上分析平台的不同

- ThreatExpert, VirusTotal, Anubis, CWSandbox
  - 提供自動化的分析報告
- 除了提供自動化分析外,此系統還提供
  - 可視可操作的VM環境
  - 直接在Web上進行Debugging
  - 先進的輔佐分析技術
    - Taint Analysis
    - Anti-anti-VM

系統功能簡介

- 檢視、修改虛擬機器的記憶體和硬碟內容
- 觀察虛擬機器網路封包
- 對程式進行單步執行，觀察暫存器、虛擬記憶體內容
- 對檔案、記憶體內容進行標記
- 將虛擬機器之被標記之硬碟磁區反轉為檔案或win registry

Debugging process in VM



File tainting and disk-sectors <--> files mapping