FATKit: A Framework for the Extraction and Analysis of Digital Forensic Data from Volatile System Memory

DFRWS 2006: Work in Progress (WIP)
Aug 16, 2006

AAron Walters

4TΦ Research

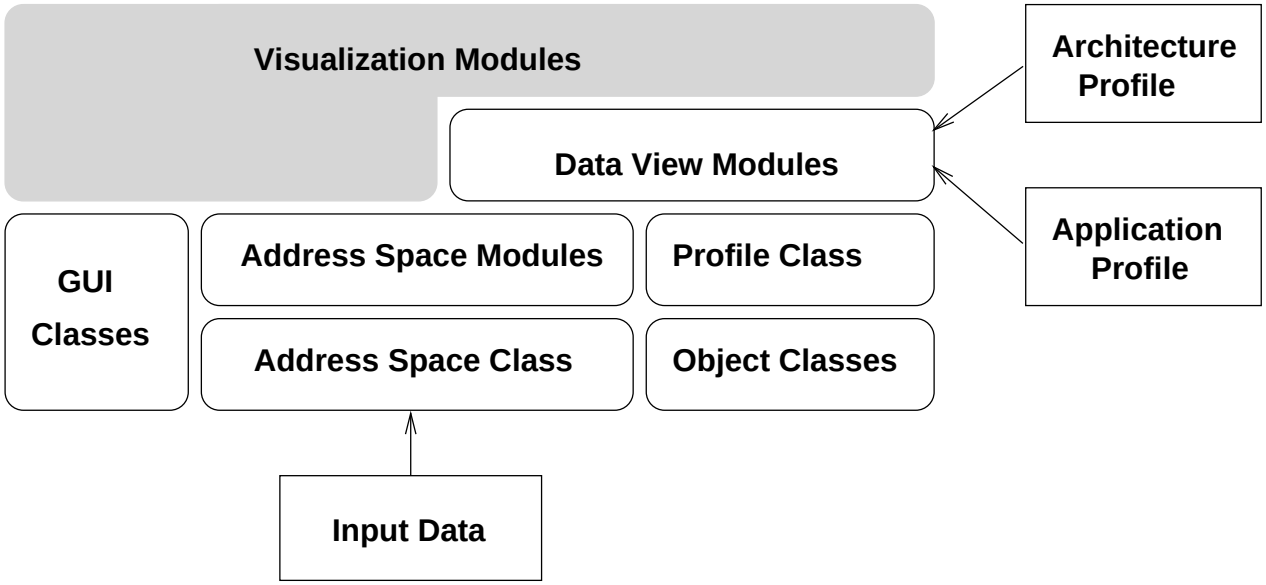
Nick L. Petroni Jr.

University of Maryland

Problem

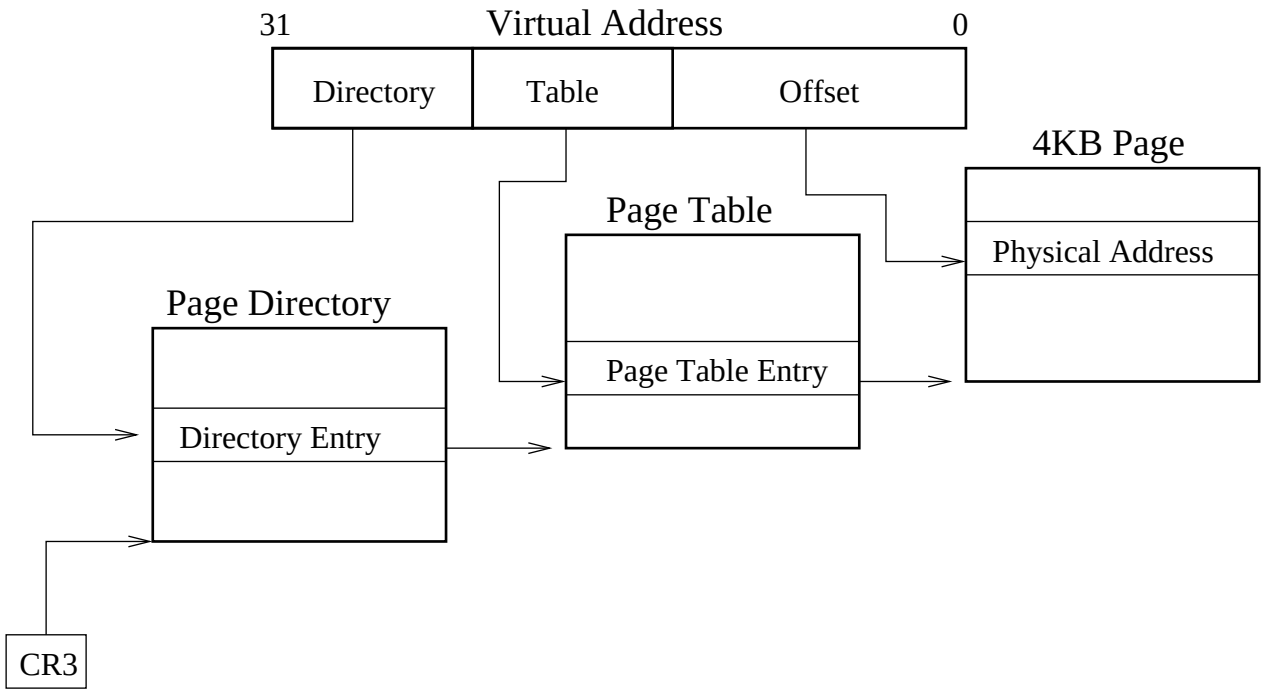
- Anti-Forensics: Meterpreter, Core Impact, Canvas
- Minimize non-volatile artifacts
- Complex and opaque information infrastructure and systems
- Runtime Integrity?
- Rootkits
- Large collections of images (crash dump, dd, etc)
- Assume malicious adversary

Forensic Analysis ToolKit



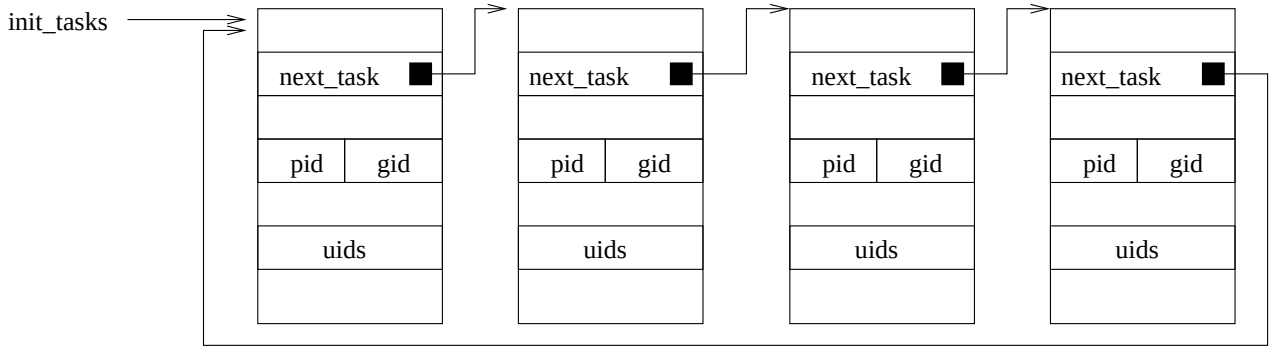
- FATKit: cross-platform, modular, extensible framework
- Extract, analyze, aggregate, and visualize
- Research: Static analysis (CIL/Ocaml), memory informatics, multi-relational data mining
- Reusability, automation, abstraction
- Advanced detection: semantic integrity predicates (Petroni,2006)

Intel IA-32 Virtual Memory Module



- Segmentation and paging
- Virtual to physical address translation
- Emulated virtual address spaces (including swap)
- Operating system independent

Linux Support



- Automatic profile generation using static analysis (CIL/Ocaml)
- Linux Kernel/User Objects: List walking and linear address space scanning (physical/virtual)
- Accumulator functions (tasks, modules, filesystem data, network sockets,etc)

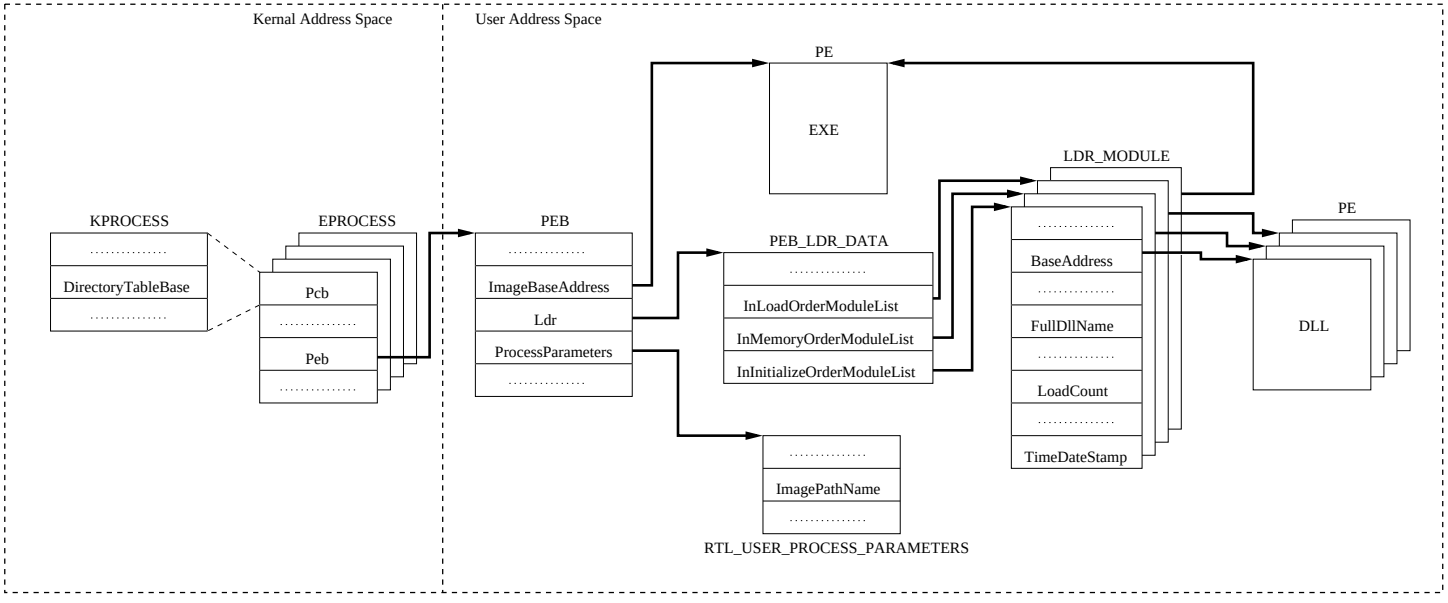
Windows Support

- Automatic profile generation (Debugging information/Binary Dissassembly): Windows 2000, Windows XP, Windows 2003 Server, Windows Vista
- Windows Kernel/User Objects: List walking and linear address space scanning (physical/virtual)
- Processes, threads, devices, drivers, etc
- PE parsing, integrity, and reconstruction (exe,dll,etc)
- Stack tracing (kernel/user)
- Enumerate Object Handles:
  - Ports, Registry Keys, Files, etc

Advanced Detection Modules

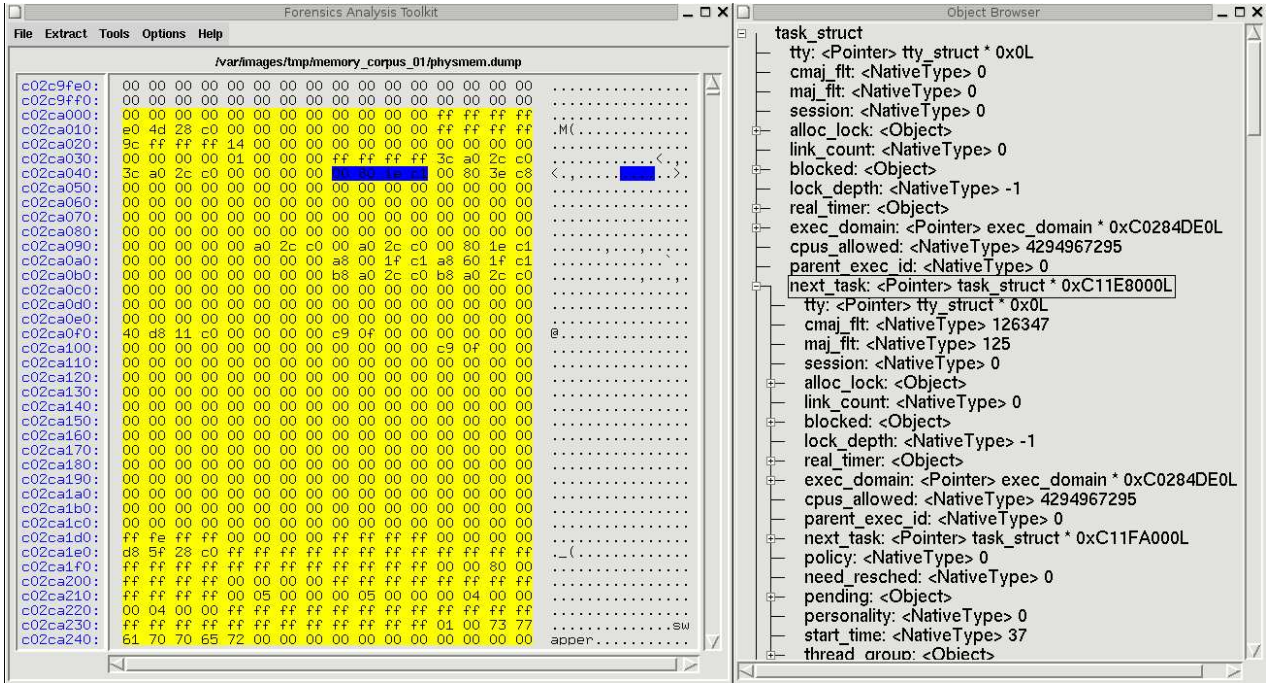
- Advanced detection data analysis module
- Kernel and userland malware (rootkits, viruses, etc)
- Injected or modified code and data
- Semantic integrity: inconsistant data conditions
  - Data hiding (DKOM)
  - Capability/access control modifications
  - Control flow modifications
- Anti-forensics techniques (contraception)
  - Example: Remote library injection

Example: Remote Library Injection



- Exploits dynamic linking of shared objects
- Correlating filesystem, memory, traffic dumps
- Semantic integrity of objects
- Extract suspicious artifacts (outlier)
- Detects public library injection attacks (Metasploit,NTIllusion,etc)

Visualization Modules



- Address Space Browser
  - Linear address space representation, color coding
- Object Browser
  - Navigate memory objects

Current Work

- Update hash databases (Trust)
- Disassembly (BinDiff, Flake)
- Hardware/Software Virtualization
  - Inside virtual machine (Blue Pill)
- Acquisition Mechanism (quantify obtrusiveness)
- Anti-forensics (Metasploit modules)
- Cross-memory analysis (Garfinkel)
- Clustering machines (rootkits,botnets)
- Xinu?
- Implemented available tools in our framework

Related Information

- Andreas Schuster: http://computer.forensikblog.de/en/
- Harlan Carvey: http://windowsir.blogspot.com
- Mariusz Burdach: http://forensic.seccure.net
- Jesse Kornblum: http://jessekornblum.livejournal.com
- FATKit: www.4tphi.net/fatkit
  - *FATKit: Detecting Malicious Library Injection and Upping the "Anti"*
- Mailing List: Volatile Memory Mailing List