Memory Forensics: A Brief Introduction

UNO GenCyber Program – July 30, 2015

Joe T. Sylve, M.S.
Senior Research Developer, Blackbag Technologies
Ph.D. Candidate, University of New Orleans

#whoami

- UNO Alumnus
  - B.S., Computer Science – 2010
  - M.S., Computer Science – 2011
  - Ph.D., Computer Science – 2016???
- Digital Forensic & Computer Security Researcher and Practitioner
  - Blackbag Technologies
  - 504ENSICS Labs
- Co-Organizer
  - NOLASec
  - BSidesNOLA

Grab a Copy of These Slides

https://github.com/jtsylve/slides

Why Memory Forensics?

- Traditional Analysis Deals w/ Non-Volatile Data
  - Hard Drives
  - Removable Media
  - Etc.
- Live Forensics Deals with Volatile Data
  - RAM Mostly
  - Must be Collected From a Running Machine
  - Not as Much Control Over Enviornment

Why Memory Forensics?

- RAM Dumps Contain Both Structured and Unstructured Information
  - Unstructured
    - Strings
    - Application Data
    - Fragments of Communication
    - Encryption Keys
  - Structured
    - Kernel and Application Structures

Why Memory Forensics?

- With This Data We Can Gather Information About
  - Processes
  - Open Files
  - Network Connections
  - "In-Memory-Only" Application Data
    - Private Browsing Mode
    - Unencrypted Data
    - Webmail
    - Etc.

Why Memory Forensics?

- Advanced Malware
- Encrypted or Temporary File Systems
- “Live” Computing Environments
- Analysis
  - Volatility
  - Rekall
  - Redline
  - Blacklight 2015 R4 (Late 2015)

How It Works

- Two Approaches
  - Signature-Based Data Carving
  - Structured Analysis
- We'll Discuss Both

Signature-Based Data Carving

- Simply Scan the Raw Memory Dump for Patterns
  - Ex. Firefox ~~Porn~~ Private Browsing History
    - Search for “HTTP-memory-only-PB”
    - Strings afterwards will be URLs
  - Can use Regular Expressions
    - Ex. Email Addresses: .*@.*\..*
- Bulk Extractor is a Good Example of This Technique

Signature-Based Data Carving

- Pros
  - Reasonably Fast
  - Easy to Implement
    - Strings, Grep, & Awk
  - Sometimes All You Need

Signature-Based Carving

- Cons
  - Not Context-Aware
    - Which Process or File?
  - Fragmented Data is Hard to Recover
    - Physical Memory is Essentially a “Random” Collection of 4KB Pages
  - Fails on Compressed Images
    - Pagefile.sys
    - OS X

Structured Analysis

- Attempts to Recreate the OS Runtime State
  - Locate Kernel
  - Parse Structured Kernel Information
  - Perform Address Translation
  - Parse All the Things!
- Tool Examples
  - Volatility
  - Rekall
  - *Blacklight (Late 2015)*

Structured Analysis

- Why the Kernel?
  - Managing Codebase of the OS
  - References Information About Everything
    - Processes
    - Files
    - Sockets
    - Drivers

Structured Analysis

- Locate the Kernel
  - Memory Dump Format
    - Crash Dump
    - Hiberfile.sys
  - Register State
    - Some Registers Point to Key Kernel Structures
  - Data Carving
    - Look for “Known Signatures” inside the kernel

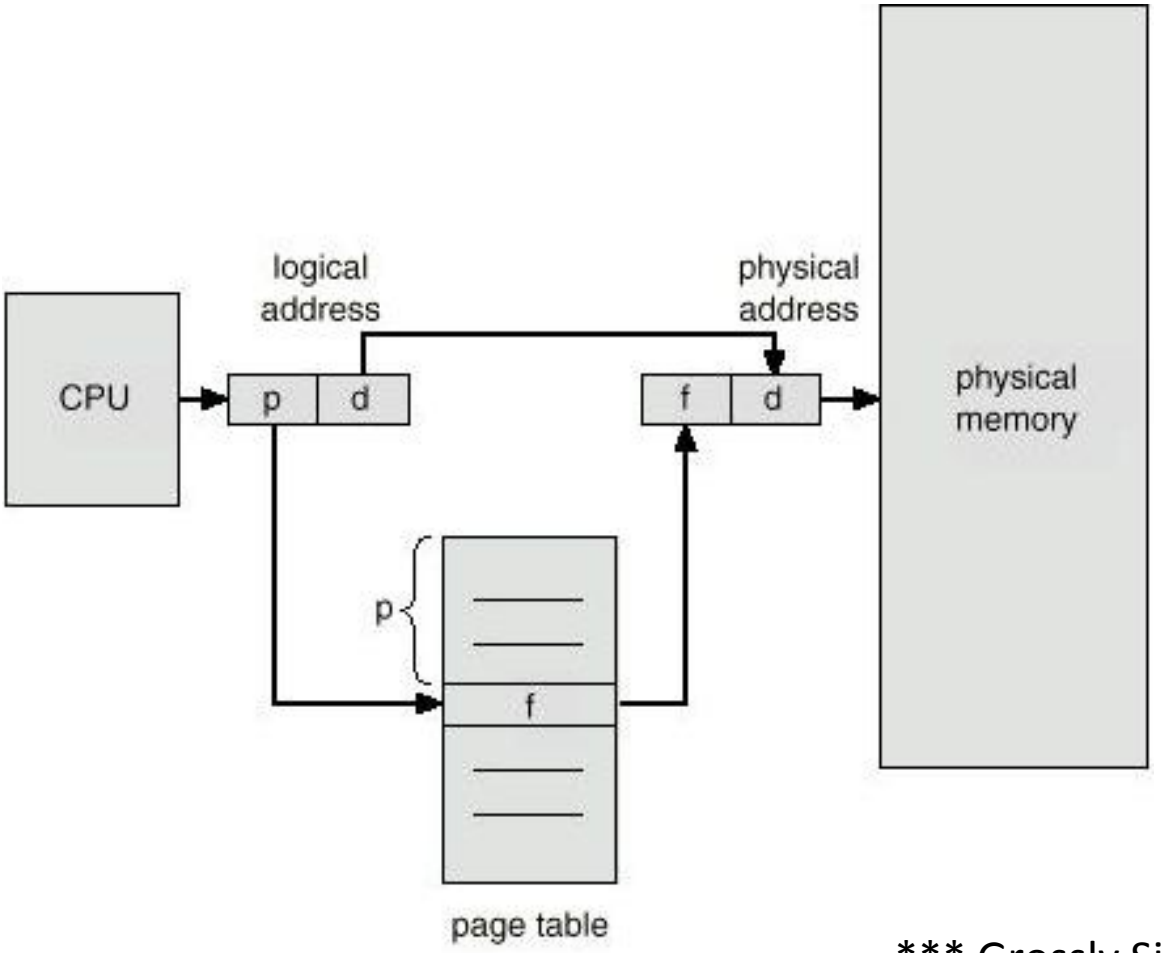
Structured Analysis

- Parse Structured Kernel Information
  - Look for Structured Data That Should Live at Known Positions in the Kernel
    - Ex. Linked List of Processes
      - nt!PsActiveProcessHead
  - Parsing This Data Will Give Us Virtual Addresses of Artifacts

Structured Analysis

- Perform Address Translation
  - Physical Memory is a “Random” Collection of Pages
    - Usually 4KB
  - Each Process Has It’s Own “Virtual Memory”
    - Linear Addresses
    - Ordered
  - Each Process Has a Table That Maps Virtual to Physical Addresses

Structured Analysis



*** Grossly Simplified

Structured Analysis

- Parse All the Things!
  - Now We Know Where Things "Live" in Physical Memory
  - We Can Look at Physical Pages "in Order"
  - Decompress (if Needed)
  - Parse Artifacts
    - Data Carving
    - Structured Application Analysis

Structured Analysis

- Pros
  - An Incredible Amount of Information Can be Found
  - Handles “Fragmented” Data Well
  - Context Aware
    - Results Can be Associated With Specific Processes, Files, and Possibly Users
  - Very Hard to Hide From

Structured Analysis

- Cons
  - Requires More Sophisticated Tools
  - Currently Available Tools Are Slow
    - This Will Change in Late 2015 ;-)

Volatility Demo (Time Permitting)

That's All for Now!

- Thoughts?
- Questions?
- Comments?

joe.sylve@gmail.com

@jtsylve

https://github.com/jtsylve/slides