Volatools: Integrating Volatile Memory into the Digital Investigation Process

AAron Walters

Nick L. Petroni, Jr.

{awalters,npetroni} [at] komoku.com

February 28, 2007

Introduction

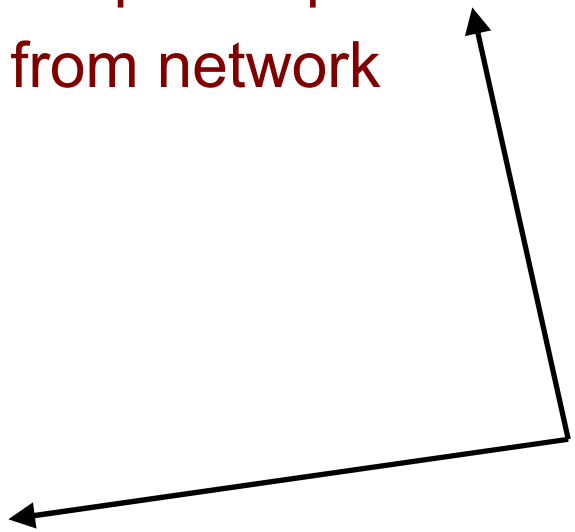
- Objectives
  - Emphasize value of memory analysis
  - Summarize state of the art
  - Help you improve your process
  - Show some demos
  - Give away free tools!
- Approach: Top-down
- Who we are
  - OS/Security researchers

Agenda

- Overview of investigative process
- Current limitations and challenges
- “Runtime state” analysis
  - Live response
  - Volatile memory analysis
- Demo tools
- Advanced techniques/anti-forensics
- Future of volatile memory analysis

Typical Scenario

1. User/admin notices sign of intrusion/crime
2. RAM dumped, live response performed
3. Machine removed from network
4. Power off
5. Image hard drive
6. Initial analysis
7. Recover/reinstall
8. Detailed analysis

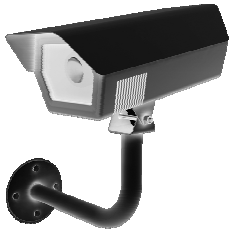


Require training and resources

Digital Investigation Process Model

- Why these steps?
- Why this order?
- Process model
  - Organize and standardize procedures
  - View the process as a whole
- Digital crime scene
  - Not just another piece of evidence
  - Many types of evidence (memory)

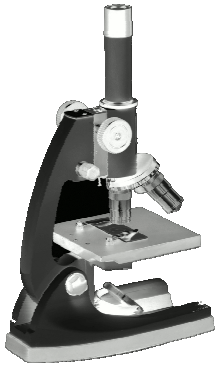
IDIP Digital Crime Scene



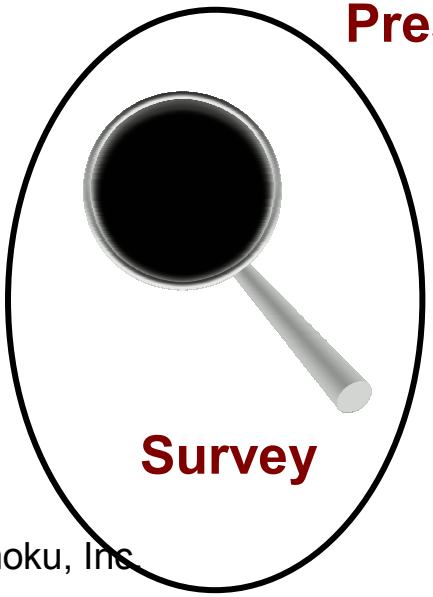
Notification

Reconstruction

Preservation



Search



Survey

“Runtime State” Analysis

- Go beyond “at rest” objects
- Analyze “in motion” state of system
- Advantage:
  - Much more context
  - Info that may be lost
- Helps with current challenges

Live Response

- What is live response?
  - Relatively new phenomenon
  - Tools/commands run on live machine
  - Provides important context and “active” state
  - Response strategy (economics, etc.)

- Typical information collected:
  - Running processes
  - Open network connections
  - Patch level/OS version
  - Network configuration
  - Open files
  - …

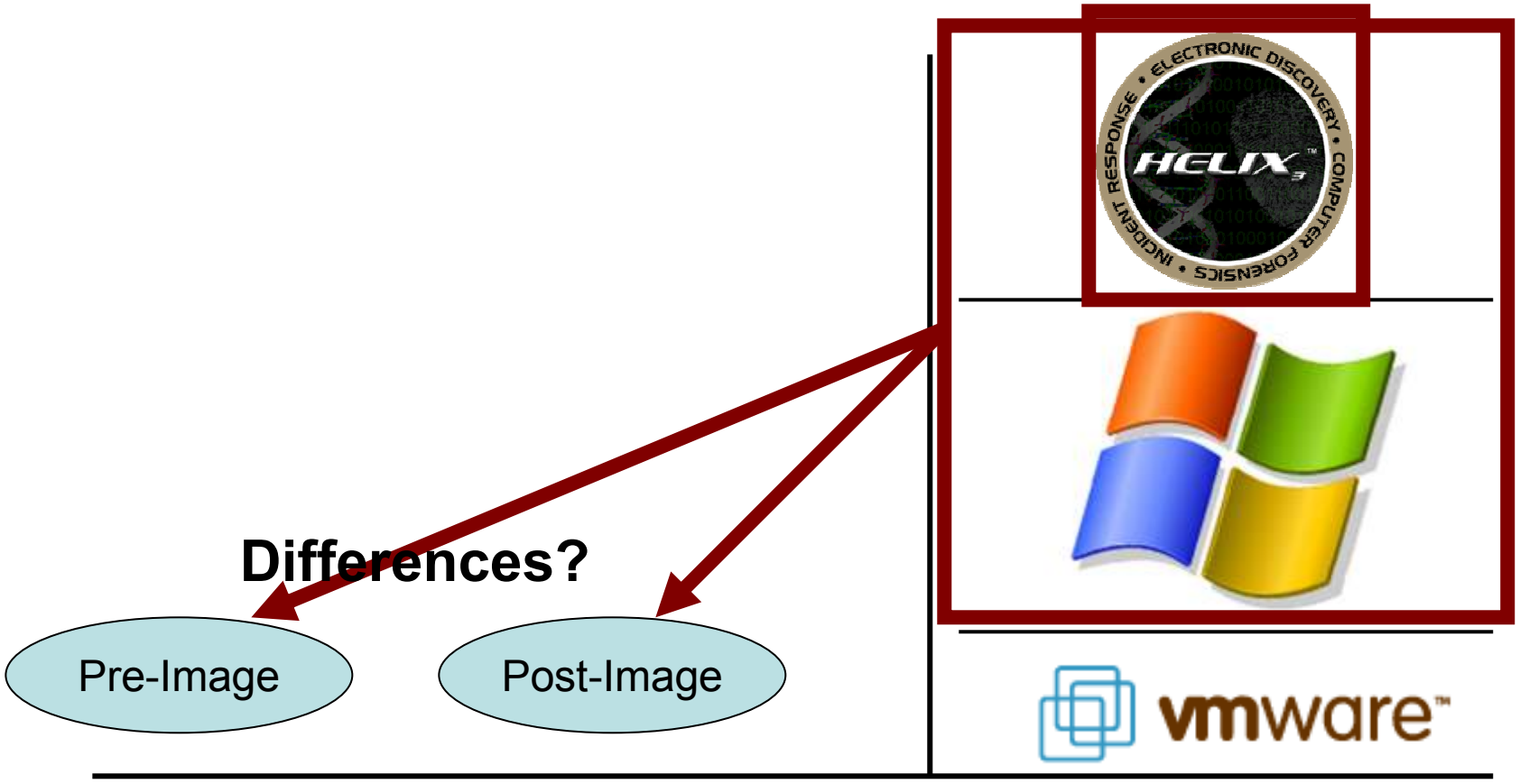
Live Response Tools

- Response toolkits
  - USB/CD Helix
  - WFT, IRCR, FRED, COFEE, RAPIER
  - SysInternals, Foundstone tools
- Commercial agent-based
  - WetStone, Guidance, Mandiant, ProDiscover

Live Response Limitations

- Live response and IDIP
  - Secure and preserve output, not raw data
- Results not reproducible
- Can’t ask new questions later
- Requires OS trust
- Impact on system
  - State, memory, swap, disk, network, etc.
  - Hard to characterize changes (but important)

Measuring Obtrusiveness



Host OS

Obtrusiveness of Collection

- Quantify impact of live response
- Metric: # bytes changed after WFT tool
- More impact than letting machine run for 15hrs

WFT

256MB	67.2%
512MB	69.4%

dd

256MB	76.9%
512MB	89.8%

Live Response

- Live response:
  - System administration tools, query the OS
  - Extra context is valuable!
  - Consider your goals/constraints carefully
  - Need to further investigate impact
  - Understand limitations
  - Take a memory dump FIRST!

Volatile Memory Analysis

- RAM contains all of the same info
- Already collected in many cases
- Instead of/addition to live response
- Helps address live response limitations

Volatile Memory Analysis

- Integration into IDIP
  - Separates data collection and data analysis
- Impact on the system
  - Reduced to a function of acquisition mechanism
- Repeatability
  - Verifiable by third party reviewer
- Asking new questions later
  - Query the original data store
- Trust
  - Minimizes trust placed in system

Public Tools and Techniques

- List-walkers/table crawlers
  - Technique: data structures act as roadmap
  - Tools: kntlist (Garner), memparser (Betz), WMFT (Burdach)

- Linear scanning
  - Technique: scan for “reliable pattern”
  - Tools: PTfinder (Schuster), lstools (Carvey), ProcessLocator (Vidas)

Volatools Basic

- Why another set of survey tools?
- What is Volatools Basic?
  - Open source (training implementation)
  - Python implementation
  - Command-line utilities
  - 32-bit Vanilla XP SP2 (no MP)
  - Provide similar info to live response
  - Operates directly on RAM images
  - Completely repeatable results

Volatools Basic

- Date and time
- Running processes
- Open ports
- Process to port mappings
- Strings to process mappings
- Process to file mappings
- Process to DLL mappings
- Open network connections

Volatools Basic

VOLATOOLS Basic DEMOS

Challenge: Volume of Evidence

- Increasing volume of evidence associated with incident (collected, stored, analyzed)
  - File systems
  - Network traffic
- Target leads
  - Context-free methods (Carrier, 2005)
- Volatile targeting
  - Triage time-sensitive data
  - Link analysis

Encryption Challenge

- Increasing use of encryption
  - Encrypted files/file systems (TrueCrypt, BitLocker)
  - Encrypted network traffic
- How do investigators deal with encryption?
  - Coercion
  - Brute force
  - etc.
- Time consuming (if successful)

Encrypted File Systems

Three guilty of identity fraud which netted millions

"In January last year Dolgov's offices were raided, but the haul would almost certainly have been much greater had not one of the gang's members, Estonian Aleksei Kostap, thrown a power switch which blanked out the bank of computers on which the operation relied and triggered layers of encryption."

David Pallister
Friday December 1, 2006
The Guardian

Volatile Memory & Encryption

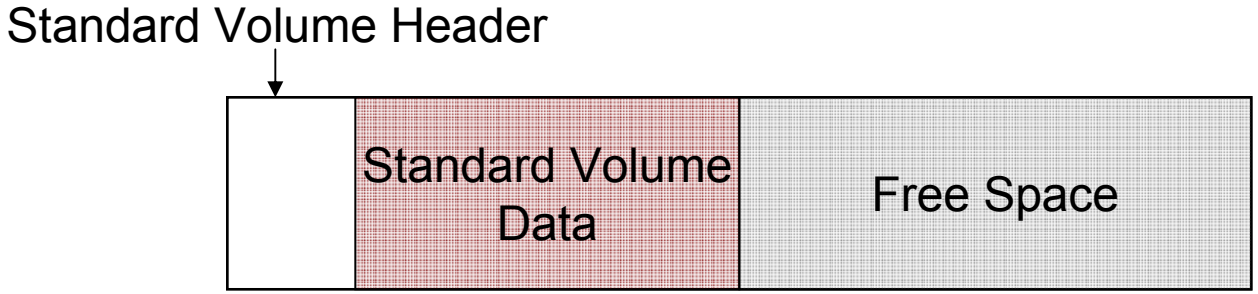
- Volatile memory analysis might:
  - Determine if encryption is being used
  - Extract volatile artifacts
- Volatile artifacts
  - Unencrypted content
  - Keying material (Klein, 2006)
  - Passwords/passphrases (Boileau, 2006)
- Keying material
  - File systems

TrueCrypt 4.2a

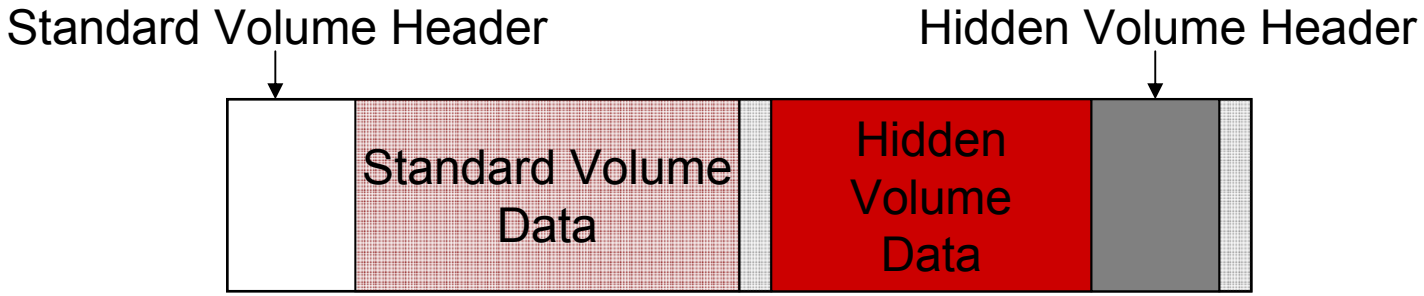
- Free open-source file system encryption
  - http://www.truecrypt.org/
- “On the fly encryption” (OTFE)
- Advanced features
  - Virtual encrypted disks (containers)
  - Cross platform
  - “Plausible deniability”
    - Hidden volumes
    - Indistinguishable volumes

TrueCrypt Volumes

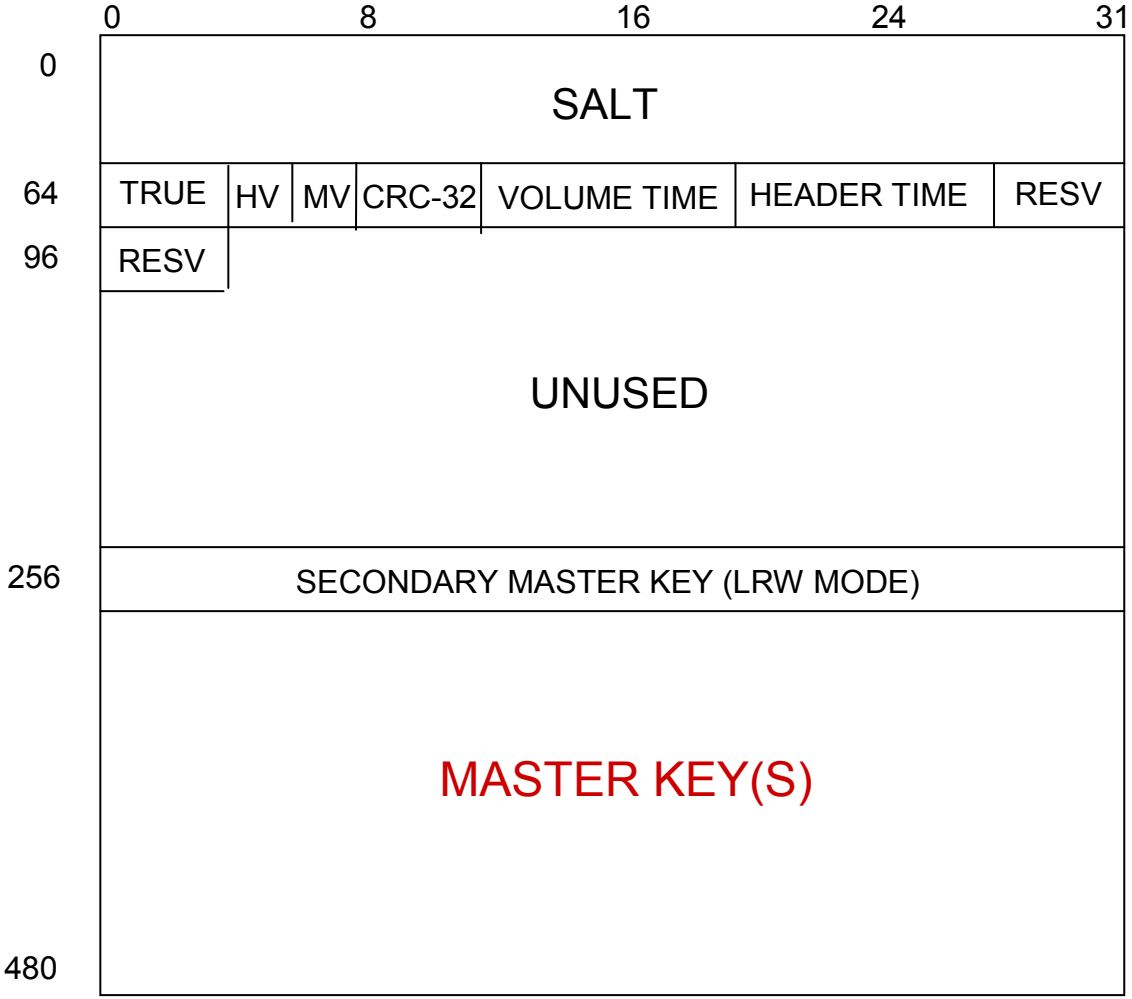
- Standard volume format



- Hidden volume format



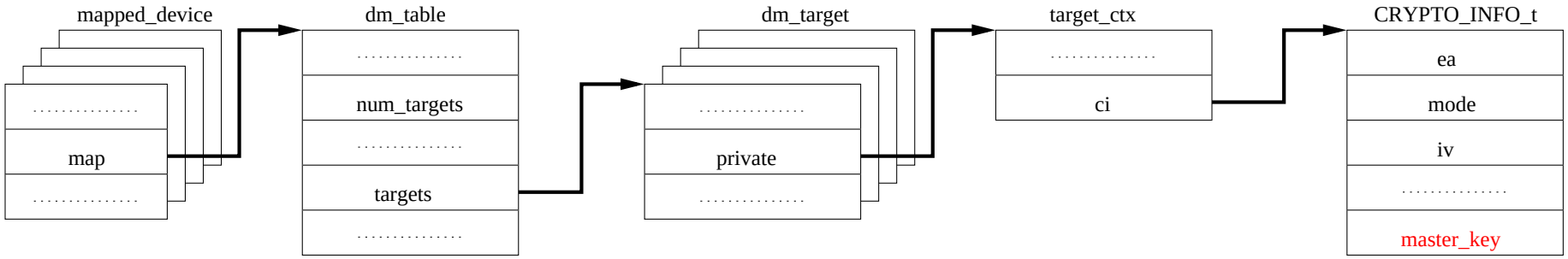
Standard Volume Header



Linux TrueCrypt

- Device Mapper target
  - Logical volume management
  - Virtual block device
- Target constructor
  - (void *) dm_target->private
  - target_ctx->ci
  - CRYPTO_INFO->master_key
- Keying material persists in RAM!!

Extracting Keys: Linux



- Major/minor numbers mapped to TrueCrypt virtual block device
- Traverse data structures to TrueCrypt context
- Extract keys!!!

TrueCrypt

TRUECRYPT DEMO

Encryption Caveats

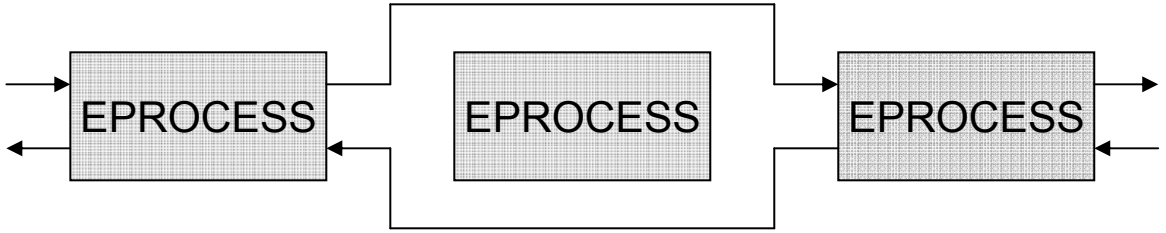
- Availability of source code
- OTFE
  - Interactive and transparent
- Kernel support
  - Linux Device Mapper: **dm_target**
  - Windows: **DeviceExtension**
- Performance
- Cryptographic principles

Challenges/Anti-Forensics

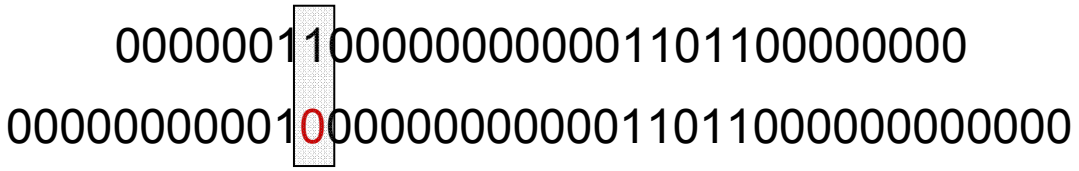
- Temporal proximity/persistence
  - Active objects
  - Non-reclaimed inactive objects (Chow, 2004)
- Blurry snapshot
  - Semantic inconsistencies
- Acquisition subversion
  - Bilby and Rutkowska
  - Virtualization and hardware

Data Hiding

- List walking techniques susceptible to unlinking (DOM)



- Linear scanning techniques susceptible to member manipulation (non-essential)



Data Decoys

- False positives/leads
  - Increase noise to signal ratio
- Context insensitive scan
- “Life-like” decoys
- Extreme: decoy operating system
  - Registers, swap, caches

Future Work

- More advanced analysis techniques
- Quantifying tool obtrusiveness
- Incorporate volatile memory analysis into your digital investigation process

Auxiliary Information

- Mailing list: Volatile memory mailing list
  - http://www.4tphi.net/fatkit
- Andreas Schuster:
  - http://computer.forensikblog.de/en/
- Harlan Carvey:
  - http://windowsir.blogspot.com
- Jesse Kornblum:
  - http://jessekornblum.livejournal.com
- Mariusz Burdach:
  - http://seccure.blogspot.com/

Contact Information

- Download Volatools Basic!
- http://www.komoku.com/volatools
- Contact:
  - awalters [at] komoku.com
  - npetroni [at] komoku.com