Carnegie Mellon
CyLab
CONFIDENCE FOR A NETWORKED WORLD

Carnegie Mellon CyLab
4616 HENRY STREET
PITTSBURGH, PA 15213
PH: (412) 268-7195
FX: (412) 268-7196
www.cylab.cmu.edu

OpenLV:

Empowering Investigators and First Responders in the Digital Forensic Process

Timothy Vidas, Brian Kaplan, Matthew Geiger

Hi, I'm Tim

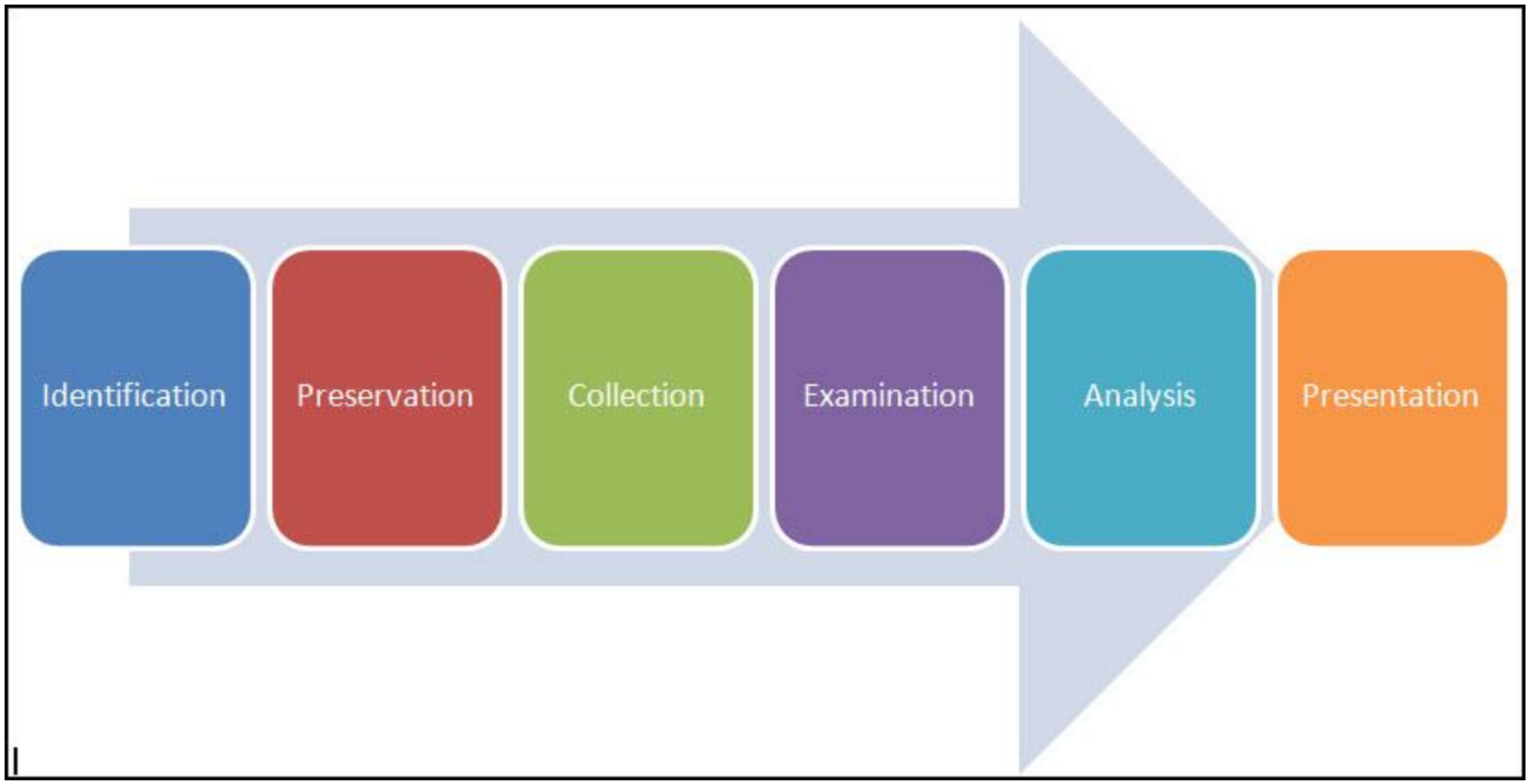
- OC member and prior DFRWS author
- PhD Candidate at CMU
- From U.S.A.

- US DoD Cybercrime Challenge champion
- DEFCON CTF winner and contest organizer

Outline

- Motivation
- The underlying issues
- Our solution
- Other applications
- Prior Work
- Conclusion

Motivation



http://aswamiariffin-cybercsimalaysia.blogspot.nl/2012_02_01_archive.html

Motivation

Consider “offline analysis tools”

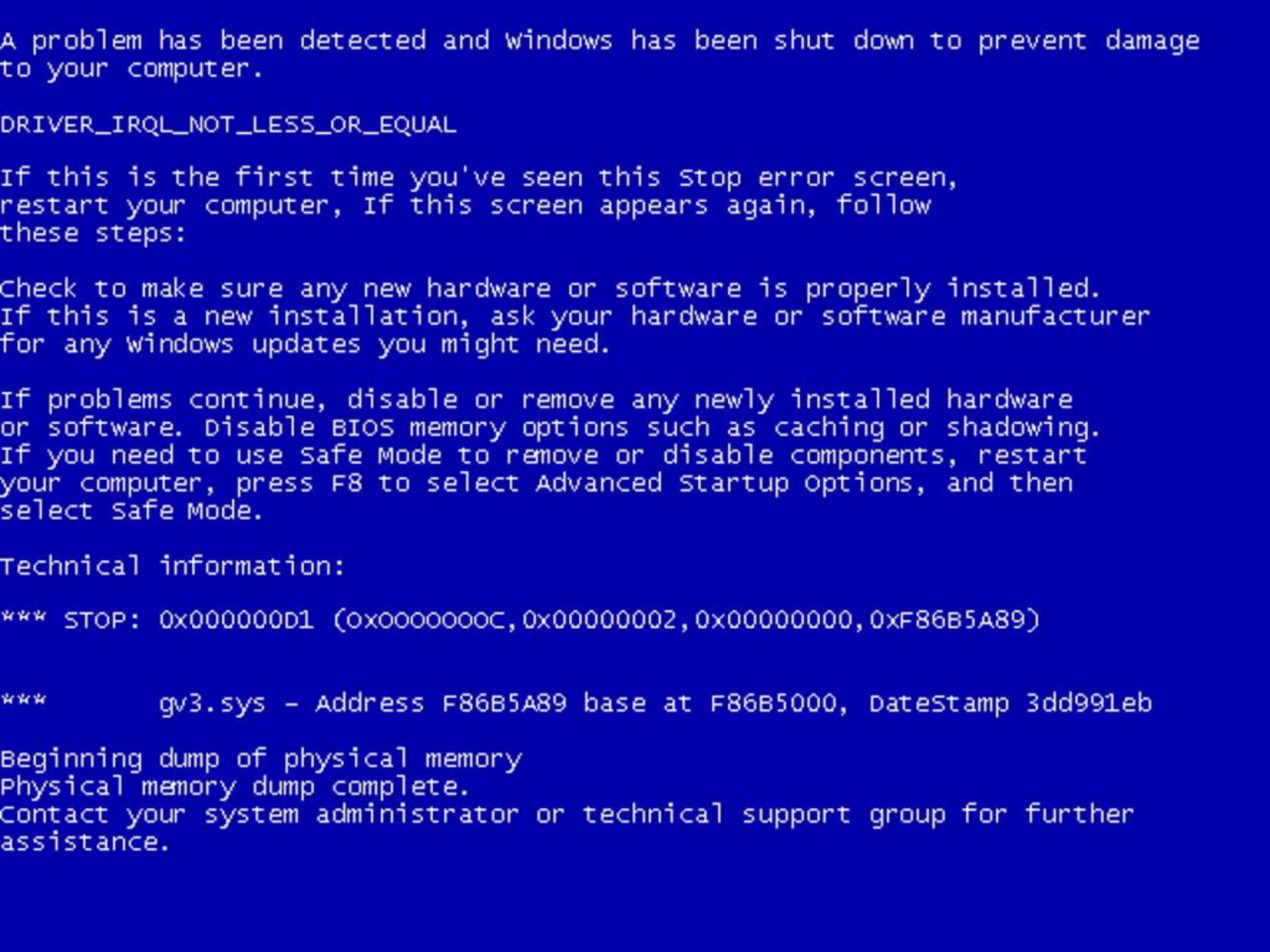
- how do you view the background image?
- how do you view the set of images that populate the vista “sidebar”?
- will Skype autostart?
- you’d like to view the Peachtree (TurboTax, etc) accounting information
  - program file (and aux files)
  - registry keys
  - activation codes (and versioning)

The Issues

- Traditional "offline" forensic analysis
  - Lose context - can't "see" the big picture
- Boot drive for "online" analysis
  - See system from the suspect's perspective
  - View proprietary/outdated data formats & software
  - Boot the system while FTK/EnCase are processing
  - Can be performed by anyone who can use a PC
- But…
  - Booting a system alters evidence
  - Need a way to use a working copy without altering it

Existing Approaches

- Physical Disk Restoration
  - Restore evidence to another physical drive
- Virtual Disk Restoration
  - Restore evidence to virtual disk drive
  - Encase PDE or Mount Image Pro
- Issues
  - Many Time Consuming Manual Steps
    - Wiping/Restoring large drives takes time
  - Hardware Compatibility
    - Drivers on image are for suspect's hardware
    - Drive size and translation issues


A problem has been detected and Windows has been shut down to prevent damage
to your computer.
DRIVER_IRQL_NOT_LESS_OR_EQUAL
If this is the first time you've seen this Stop error screen,
restart your computer, If this screen appears again, follow
these steps:
Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.
If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.
Technical information:
*** STOP: 0x000000D1 (0x0000000C,0x00000002,0x00000000,0xF86B5A89)
*** gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb
Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.

In Summary

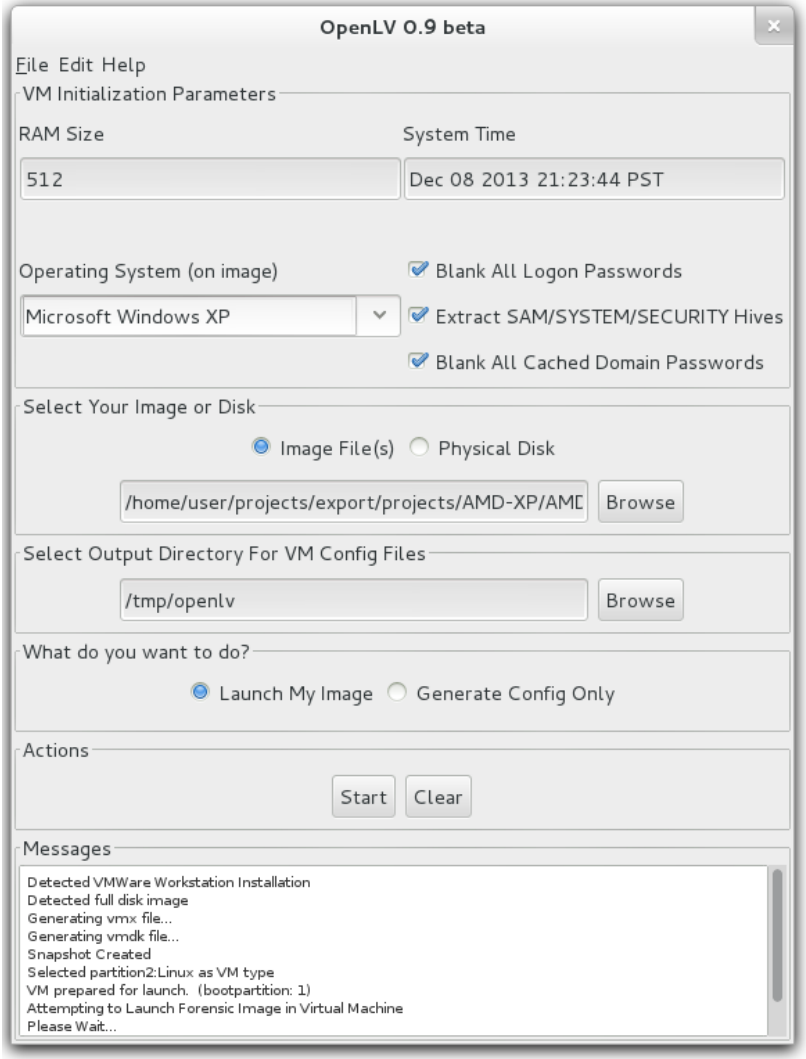
- Existing approaches are some combination of:
  - Difficult
  - Time Consuming
  - Risky
  - Expensive

All are prone to boot failure a significant percentage of the time

- Due to hardware incompatibility
- Infamous “blue screen of death”

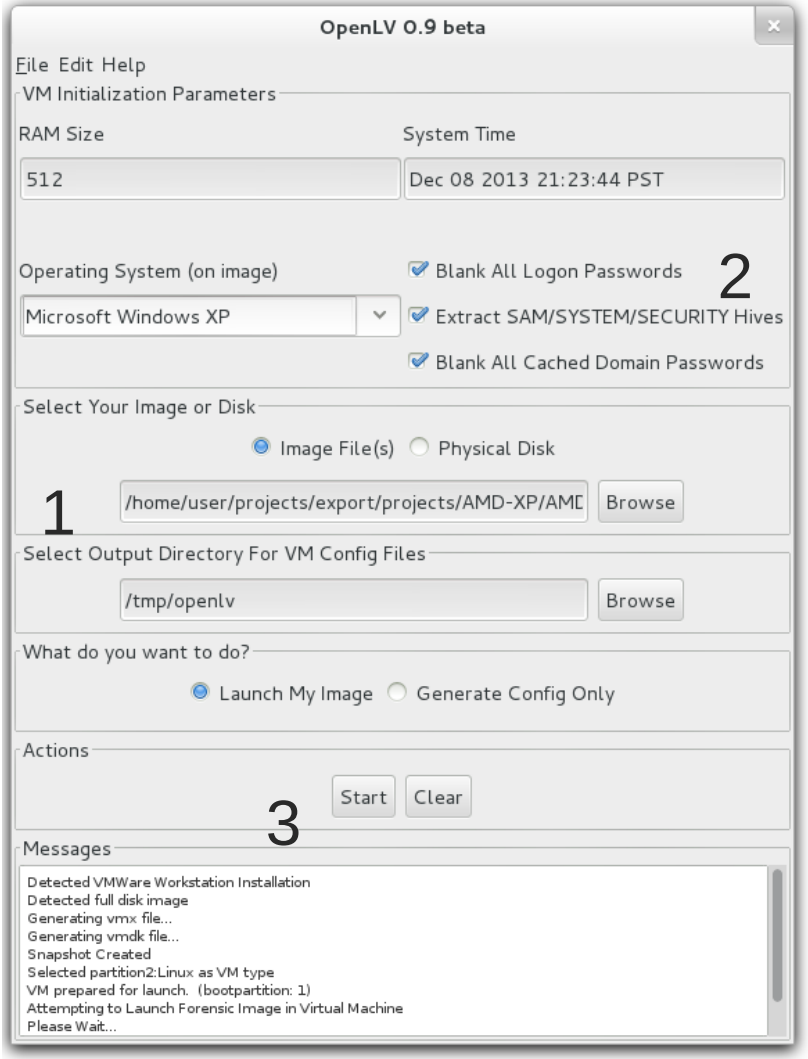
A Better Way

- OpenLV
  - Boot “bit-for-bit” disk image in VM window with a few clicks
  - No lengthy disk restoration required
  - Image is not altered in any way (can even be read-only or hardware write-blocked)
  - Automates troubleshooting process of preparing image to boot on new hardware
  - Free and freely available
    - Works with VirtualBox or VMware
    - Works with Linux or Windows exam computers
  - Open source
    - openlv.org



A Better Way

1. Select source material (aka evidence)
2. Adjust parameters (OpenLV will populate default values)
3. Click “start” to launch a VM backed by collected images

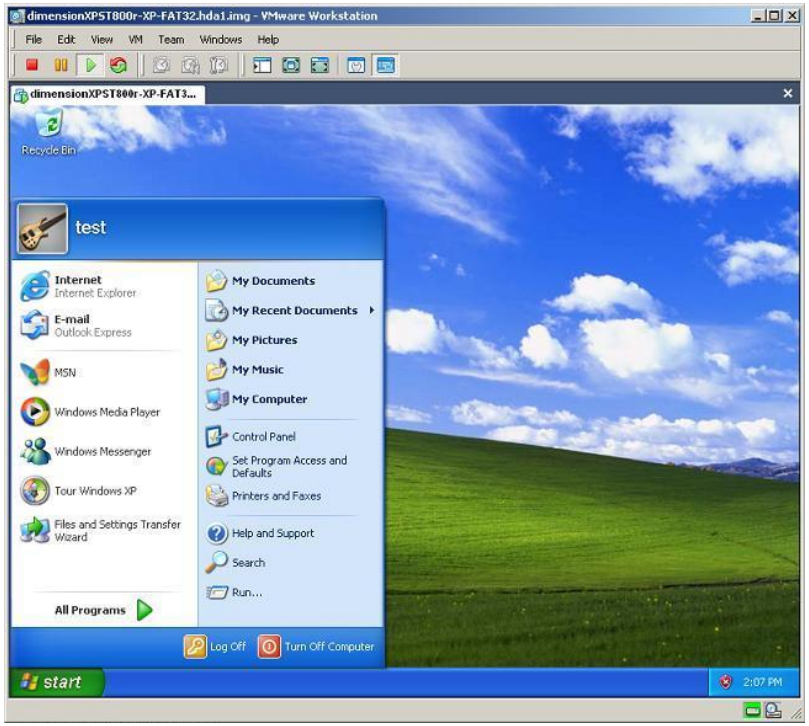


Behind the scenes

- OpenLV then:
  - Creates a virtual disk which has data areas mapped to the collected (“evidence”) data
  - Creates a snapshot of this virtual disk so that VM modifications do not affect the collected data
  - Injects software to support virtual hardware, preventing BSOD

Under the covers

- Partition Images
  - Synthesizes appropriate MBR
- Set System Time
  - Time sensitive software
- Instantly Revert to Original
  - No re-imaging required
- Ethernet Card Disabled
- Split (Chunked) Image Support
- Password blanking
  - Extraction for cracking (SAM/SYS)
  - Including Cached Domain Creds



OpenLV Supports

- Physical disks
  - Also via write blocker
- “dd-style” (raw) forensic Images
  - Windows (8, 7, 2008, Vista, 2003, XP, 2K, NT, Me, 98)
  - “Limited Support” (Linux, FreeBSD, Other)
  - Can be “split”
  - Other types are supported through third-party software (e.g. mount image pro)
- Virtualization Software (on examination host)
  - VMware Workstation 5.x – Current
  - VMware Server 1.x (Free)
  - VirtualBox 4+

Other Applications?

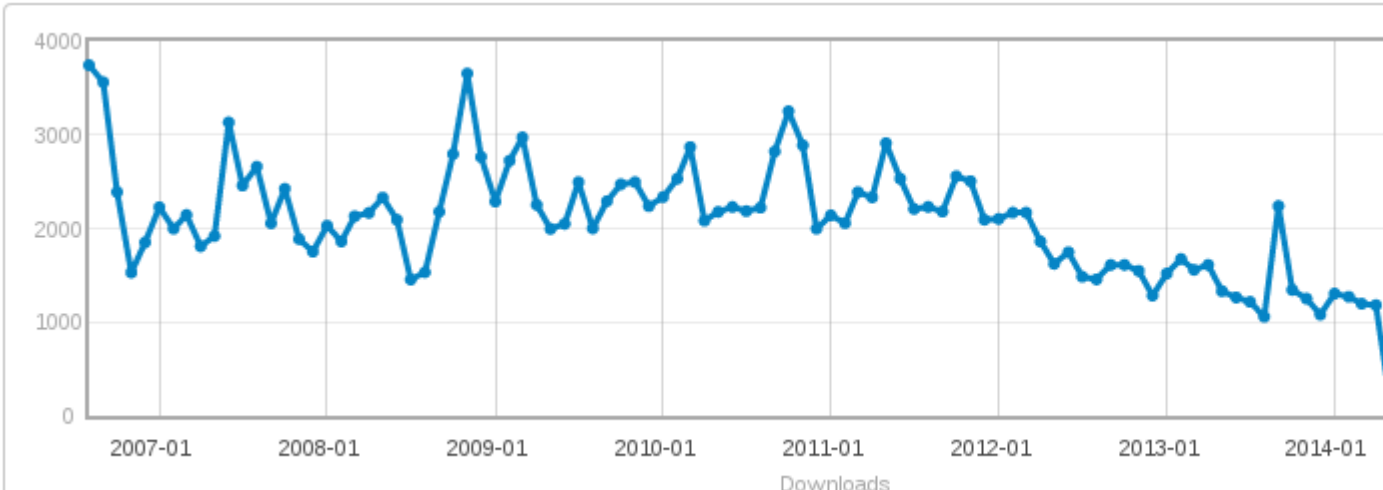
- Not Just For Forensic Analysis
  - Lab or Training Tool
  - Analysis by experts in non-forensics areas (eg accounting)
  - Court demonstrations
    - Boot the image
    - VMware video capture
    - VMware screen capture
  - Incident Response
    - Safe way to do a quick examination of an image
  - Field Forensics
    - Lightweight and portable forensics lab

Motivation (revisited)

- Obviously OpenLV was born from LiveView
- Desire for LiveView to be “more open”
  - Odd distribution model
  - People don’t know that a “private” or “law enforcement only” version exists
  - Development pace unknown and in new directions
  - Windows and VMware only

LiveView's success

- Used in unanticipated use-cases
- Others present on LiveView at digital forensics conferences
- People seem to actively use it
  - Help and new version requests
  - Continued downloads despite no new versions



OpenLV Summary

- It's advantageous to be able to see and interact with a machine from the suspect's point-of-view
- Doing so without contaminating evidence can be a tedious process
- Tools like OpenLV make such tasks trivial
  - Can make forensic investigations more efficient
  - Presentation of evidence more effective

Questions?

tvidas@cmu.edu

@tvidas

openlv.org

github.com/tvidas/OpenLV/