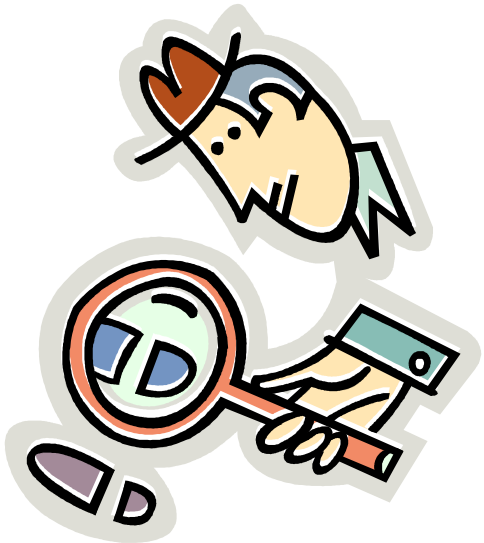
# Virtualização e Computação Forense

## You Shot The Sheriff 4 – Maio/2010

Tony Rodrigues, CISSP, CFCP
inv.forense arroba gmail ponto com

# Quem sou ?

- Tony Rodrigues, *CISSP, CFCP, Security+*
- Gestor/TI e Consultor em Segurança de Informações
- Perito/Investigador em Computação Forense
- Blog: http://forcomp.blogspot.com



# Agenda

- Introdução
- Adaptando Técnicas
- Virtualização e Computação Forense
- Forense em Máquinas Virtuais
- Máquinas Virtuais como ferramentas de Investigação
- Máquinas Virtuais X Peritos
- Conclusão

# Máquinas Virtuais

- Usa software para emular o hardware
- Um host pode ter várias máquinas virtuais sendo executadas
- Vários sistemas operacionais diferentes coexistindo no mesmo host
- Facilidade de backup e restore
- Otimização do processamento
- Setup prático e rápido

A praticidade também pode ser usada contra você !

# As mais conhecidas






Windows Server 2008
Hyper-V™

## Basicamente ...

- Possuem uma console para gerenciamento das VMs
- As VMs são arquivos (Configs, Memória e Disco)
- Permitem dar “pause” em uma VM
- Permitem descartar modificações feitas depois de um ponto de marcação
- Permitem adicionar devices virtuais que se conectam aos devices reais do host

# Nas Corporações

- Grande aumento no uso de servidores virtualizados
  - Redundância de serviços
  - Ambientes de homologação
  - Concentração de servidores com baixa carga de processamento
  - Apoio em estratégias de recuperação de desastres
  - Separação de camadas
  - Distribuição de appliances virtuais

# Mudança de cenário implica ...

de técnicas e ferramentas

**Adaptação !**

# Virtualização na Computação Forense

- Forense em Máquinas Virtuais
- Máquinas Virtuais como ferramentas de Investigação
- Máquinas Virtuais X Peritos

# Forense em Máquinas Virtuais

- O ambiente de investigação é composto por uma ou mais máquinas virtuais
  - Operação de Dead Acquisition é mais rápida;
  - Possibilidade de Operação de “semi-live” Acquisition;
  - Memory Acquisition muito mais simples e rápida;
  - Possibilidade de live analysis sem modificações (uso do snapshot em produção)

# VM como ferramenta forense

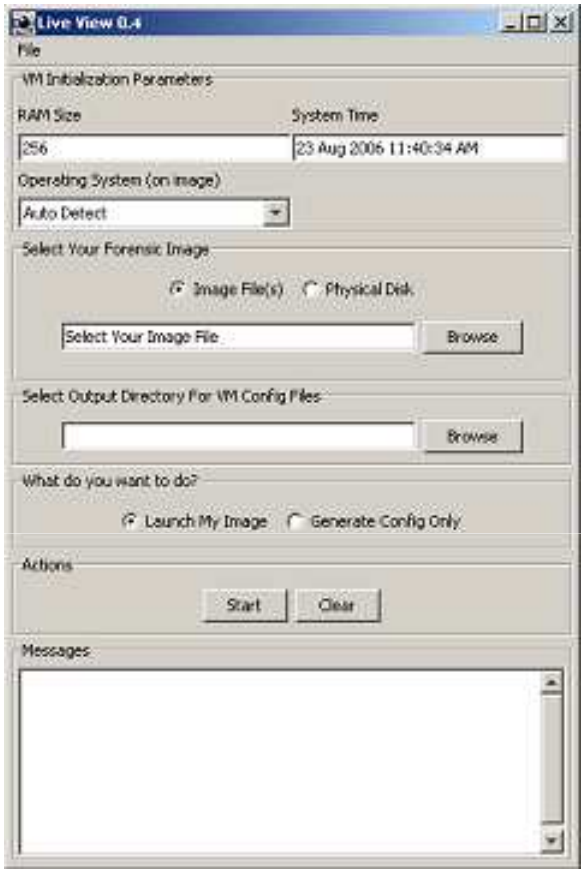
- Forense de Malware
- Análise dinâmica de imagem forense
- Pesquisa de Artefatos
- Appliances Virtuais

# VMs em Malware Forensics

- Análise de Malware
  - Reengenharia x Tempo
- Análise Estática x Análise Dinâmica
- Uso de VMs na Análise Dinâmica de Malware

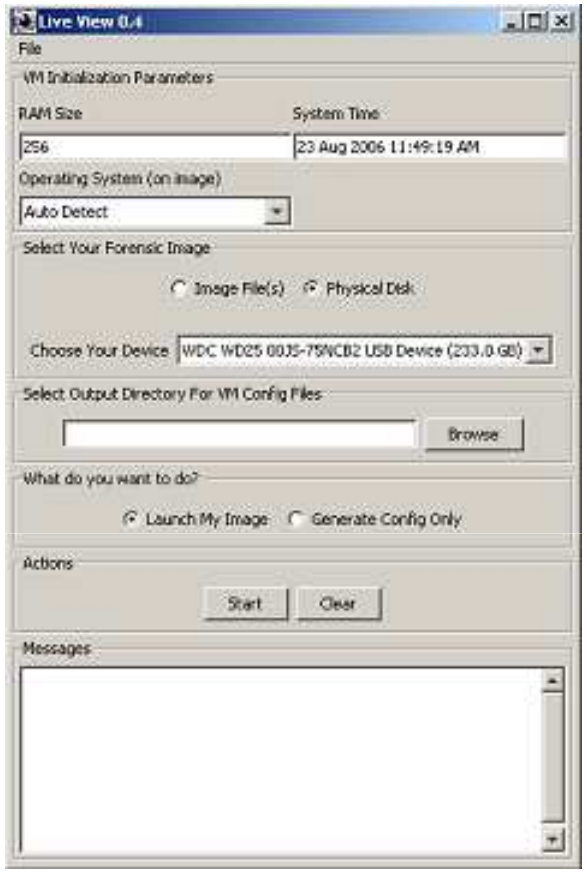
# VMs na Análise Dinâmica de Imagens Forenses

- Imagens Forenses – Dead Analysis
- Análise Dinâmica de Imagem Forense
  - Inicialização pela imagem
  - Abordagem “Read-Only”
  - Perspectiva do Usuário
  - Ferramentas disponíveis
- LiveView
  - Projeto da Carnegie Mellon University
  - Cria uma VM compatível com o VMWare



# VMs na Análise Dinâmica de Imagens Forenses - II

- Possibilidade de uso em Resposta a Incidentes e Live Analysis
  - LiveView permite criar VMs para discos rígidos da máquina
  - Read-Only
  - Pode ser usado em conjunto com F-Response para minimizar interações com o ambiente comprometido



# VMs na Pesquisa de Artefatos

- Perícia == Análise de Artefatos (Vestígios)
- Testes para determinar artefatos
  - Preparar a máquina demanda muito tempo
  - Vários SOs
  - Máquina precisa ser desmontada ao final
- Máquinas Virtuais resolvem o problema

# Appliances Virtuais para Forense

- Máquinas Virtuais pré-configuradas
  - Softwares específicos
  - Automount, swap, Journaling e outras funcionalidades desligadas
  - Facilidade de distribuição
  - Melhor opção do que Live CDs para ferramentas baseadas em bancos de dados
    - PyFlag
    - PTK
- SANS SIFT
- VM Brasileira para Computação Forense

# Máquinas Virtuais X Peritos

- VMs específicas para atividades maliciosas
  - Os vestígios diretos ficam todos dentro de um mesmo container
  - Wipe do container == Adeus vestígios
- Peritos ➔ Pensamento 3D !
  - Evidências não estão apenas no HD
  - Corolário de Harlan Carvey:

    “Ausência de evidências é uma evidência”
  - Vestígios de presença de VMs no host

# Conclusão

Virtualização cresce em utilização e esse crescimento traz, a reboque, a necessidade de adaptação do Perito em Computação Forense às novas potencialidades e ameaças.

# Referências

- F-Response
  - http://www.f-response.com/
- Live View
  - http://liveview.sourceforge.net/
- SANS SIFT
  - https://computer-forensics2.sans.org/community/downloads/
- PyFlag
  - http://www.pyflag.net/cgi-bin/moin.cgi
- PTK
  - http://ptk.dflabs.com/
- QEmu
  - http://www.qemu.org/
- VMWare
  - http://www.vmware.com/

QEMU
open source processor emulator


PTK

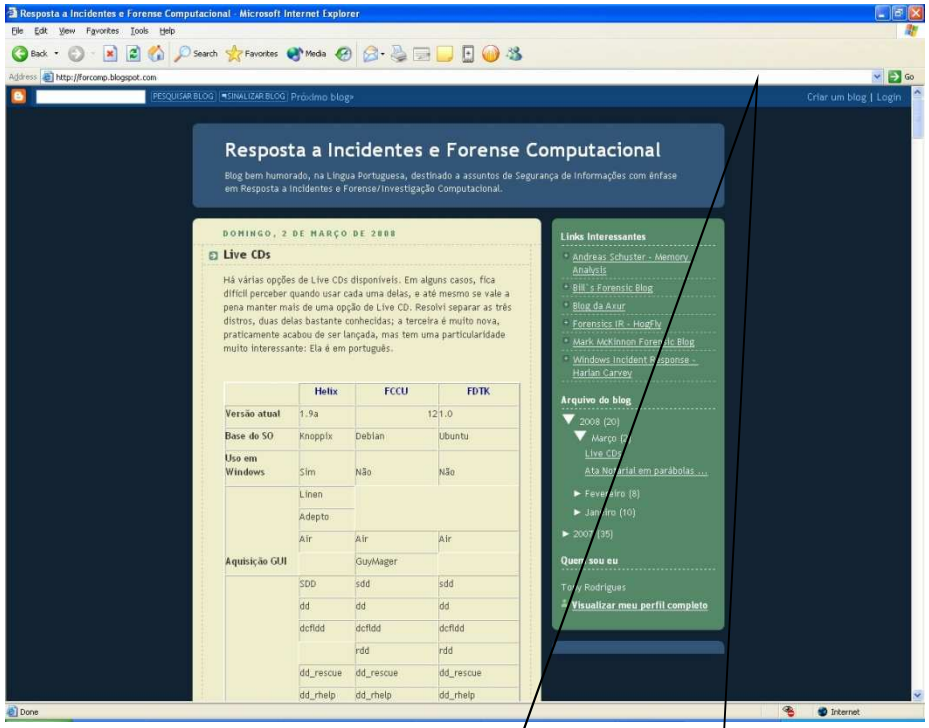
F-Response

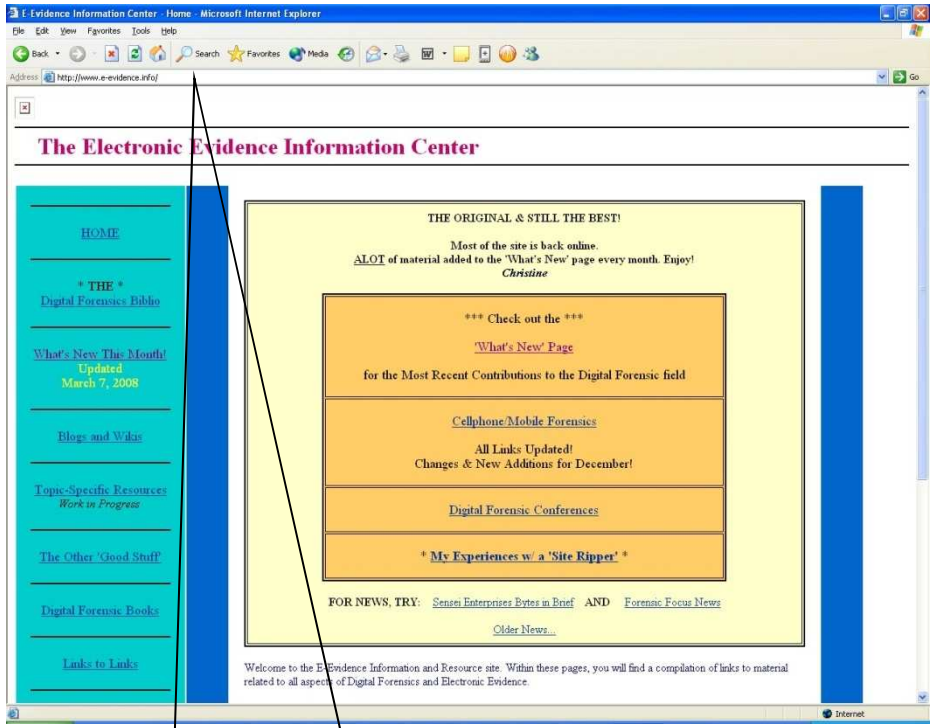
# Referências II

- XEN
  - http://www.xen.org/
- Virtual Box
  - http://www.virtualbox.org/
- Virtual PC
  - http://www.microsoft.com/windows/virtual-pc/
- Hyper V
  - http://www.microsoft.com/windowsserver2008/en/us/hyperv-main.aspx




# Sugestões de Leitura




http://forcomp.blogspot.com

http://www.e-evidence.info

# Obrigado !


inv.forense arroba gmail ponto com

(Tony Rodrigues)