Análise de Artefatos Maliciosos

Angelo Carlos M. Carvalho[12] Dario S. F. Filho[12] Luiz Otávio Duarte[1] Marcelo Carvalho Sachetin[1] Antonio Montes[1]

[1]CenPRA - Centro de Pesquisas Renato Archer
DSSI - Divisão de Segurança de Sistemas de Informação
[2]Unicamp - Universidade Estadual de Campinas
IC - Instituto de Computação

Outubro 2007

Índice

Índice

O que são

Também conhecidos como malwares (malicious software), artefatos maliciosos são programas destinados a executar em um sistema de forma ilícita com o intuito de causar algum dano.

Tipos de artefatos maliciosos:

- Vírus
- Worms
- Trojan horses
- Spywares
- Bots
- Backdoors

Danos que causam

- Roubo, perda ou alteração de informações
- Paralizasão de um serviço prestado
- Manipulação da máquina infectada
- Perda de arquivos ou de desempenho do computador e da rede

Danos que causam

- Artefatos maliciosos geraram perdas estimadas de cerca de US$ 13 bilhões devido a perda de produtividade e queda de receita gerada por sistemas indisponíveis em 2006 em empresas de todo o mundo. (IDG Now! - 13 de junho de 2007)

Como se propagam

- Através de pastas compartilhadas em rede
- Arquivos em mídia removível
- Arquivo anexo em e-mail ou contido em alguma página da Internet
- Através de uma vulnerabilidade explorada de uma determinada aplicação

Crescimento no número de ataques

- Número de crackers que roubam contas bancárias cresceu 81% em relação ao ano passado devido a utilização de artefatos maliciosos (Info Online - 03 de agosto de 2007)
- Vírus para dispositivos móveis crescem mais de 1.200% em três anos (IDG Now! - 15 de junho de 2007)

Índice

Projetos

- Desenvolver métodos de coleta automatizada de artefatos maliciosos
- Desenvolver um ambiente de análise
- Gerar relatórios e fazer a classificação dos artefatos com base no resultado da análise
- Pesquisar por tecnologias utilizadas nos artefatos capturados

Finalidade

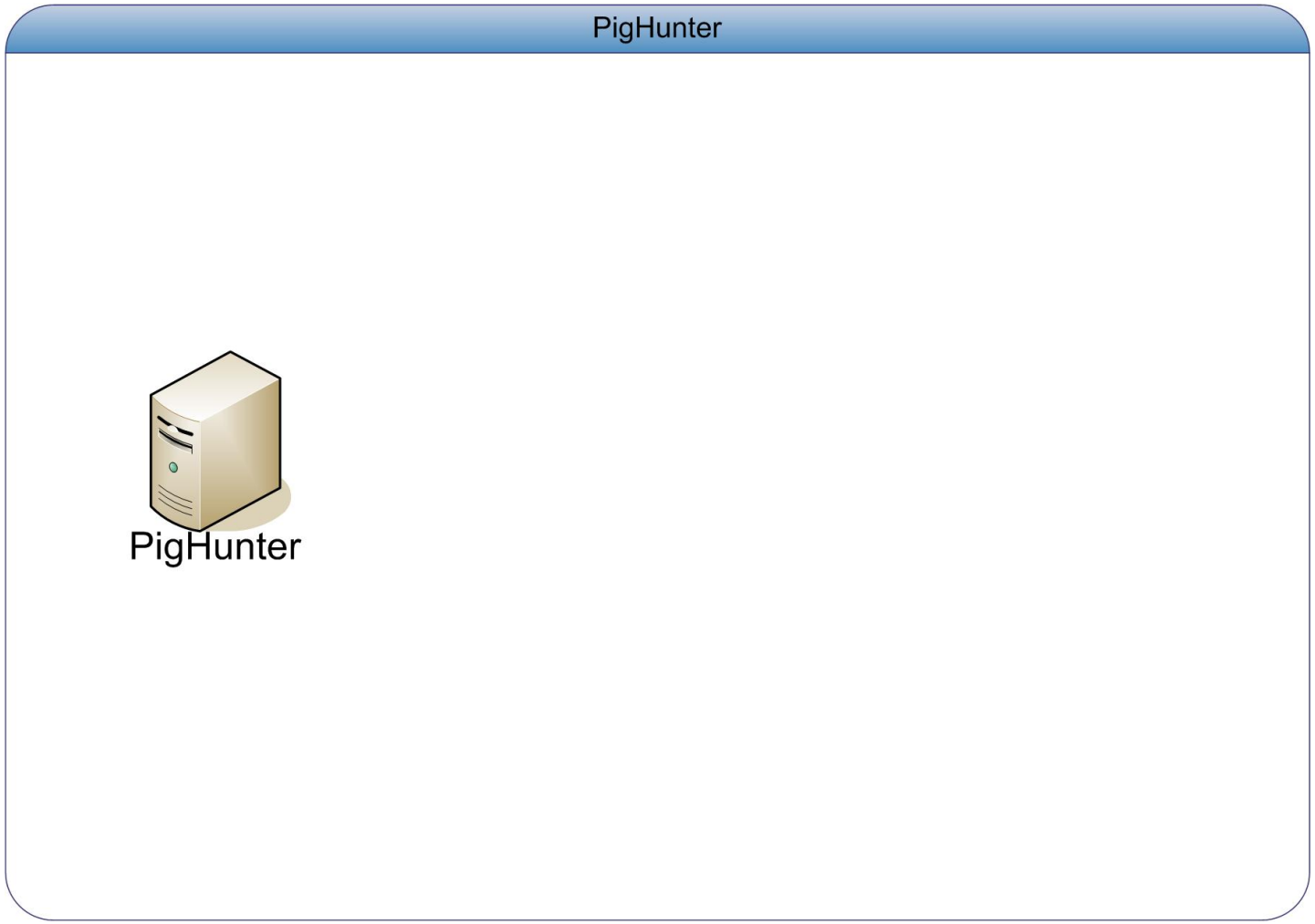
- Identificar os objetivos dos artefatos atuais, afim de descobrir os danos que podem causar
- Analisar o comportamento dos artefatos, para descobrir formas de como evitar suas ações
- Desvendar as técnicas utilizadas, para evitar que elas funcionem

Índice

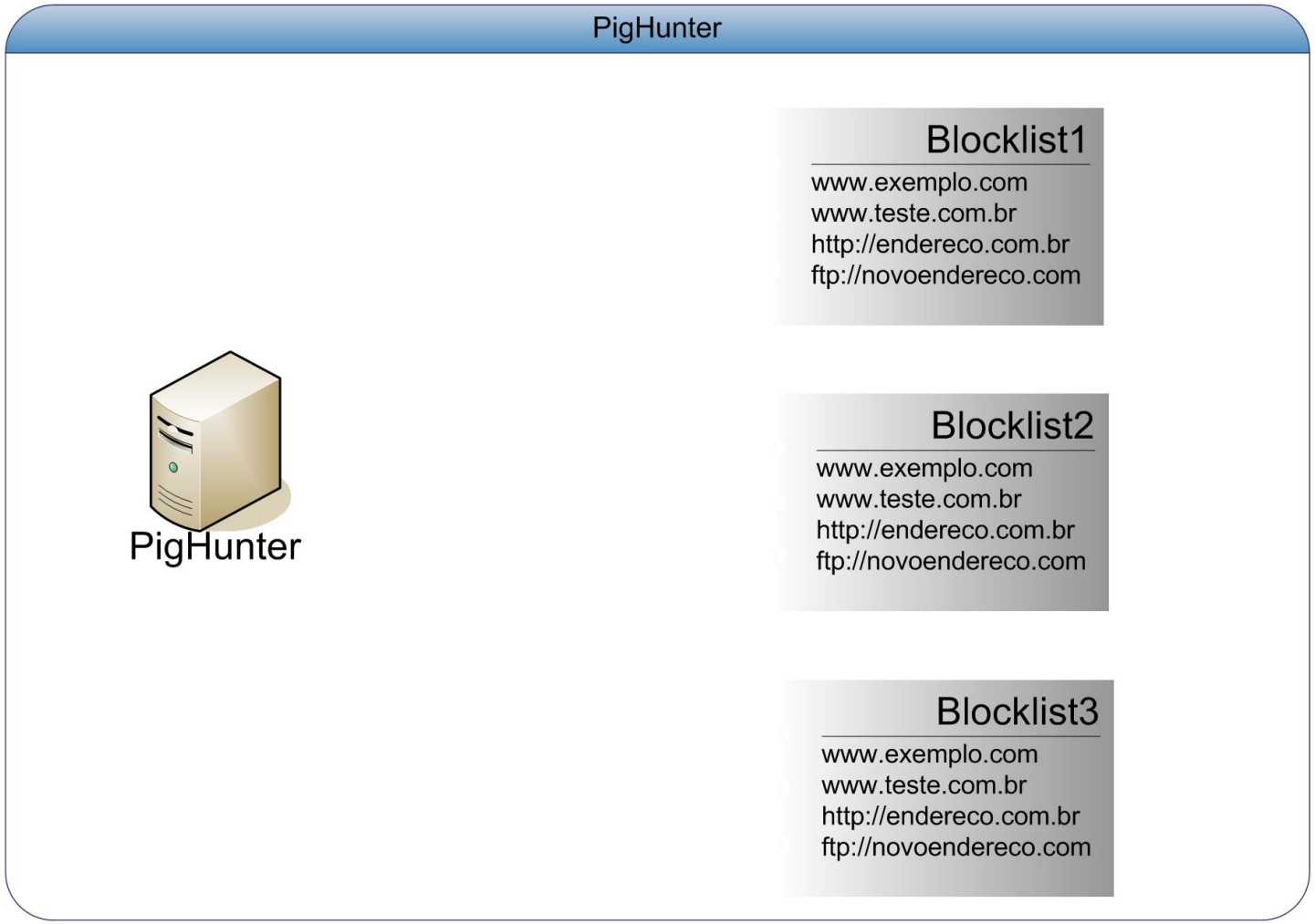
Metodologias

- Via Blocklists
- Via SPAMS
- Através da honeynet

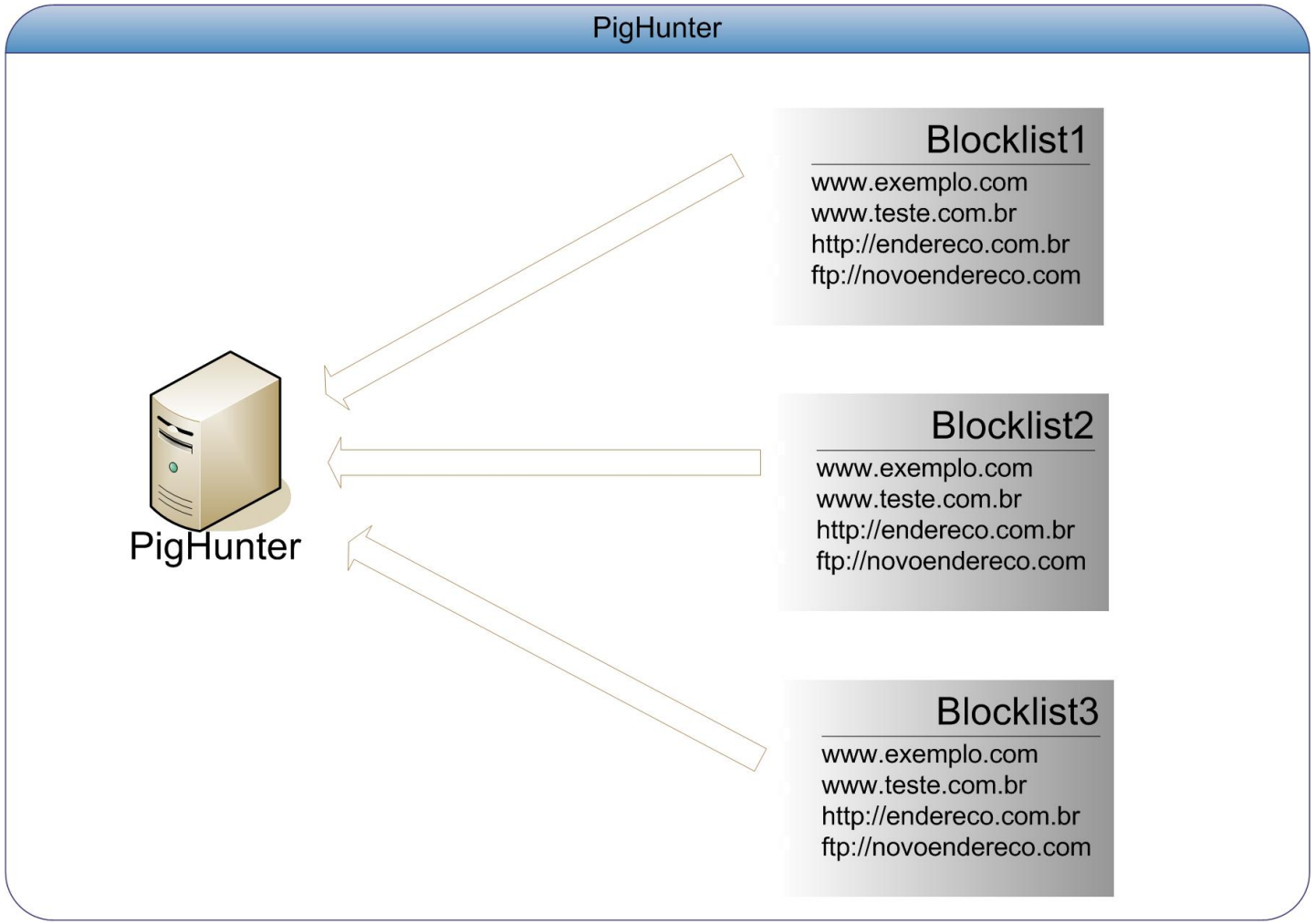
Via Blocklists



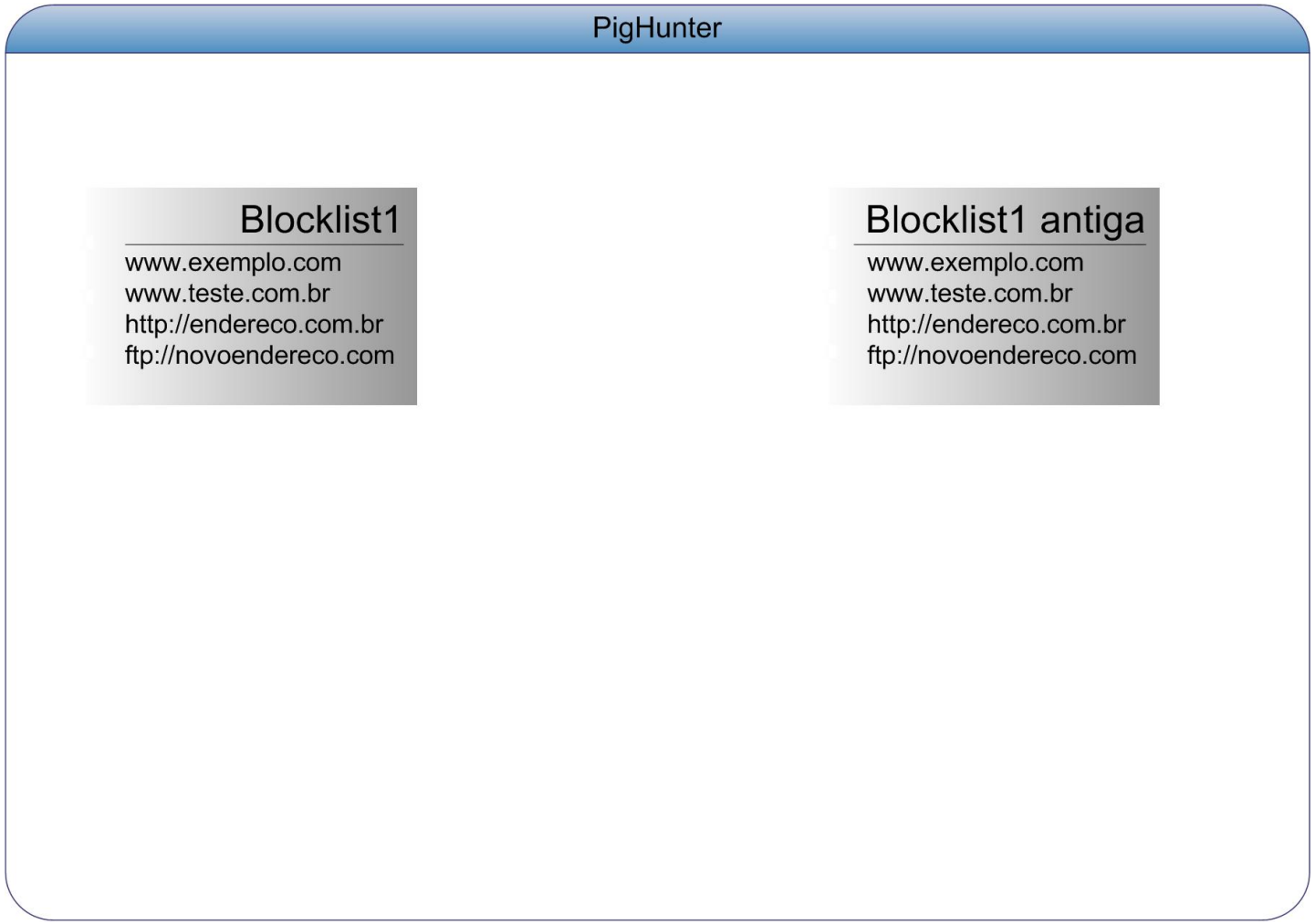
Via Blocklists



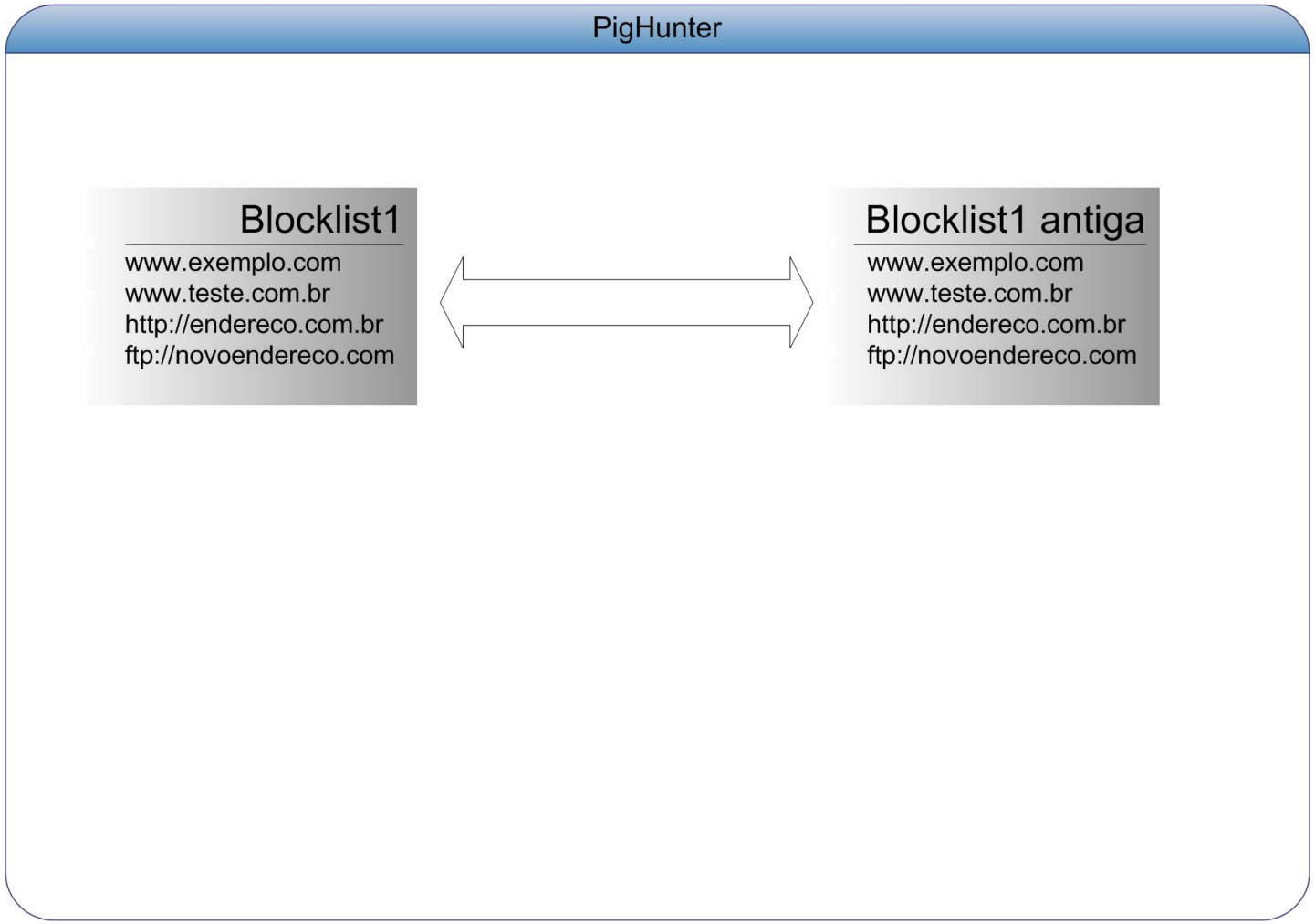
Via Blocklists



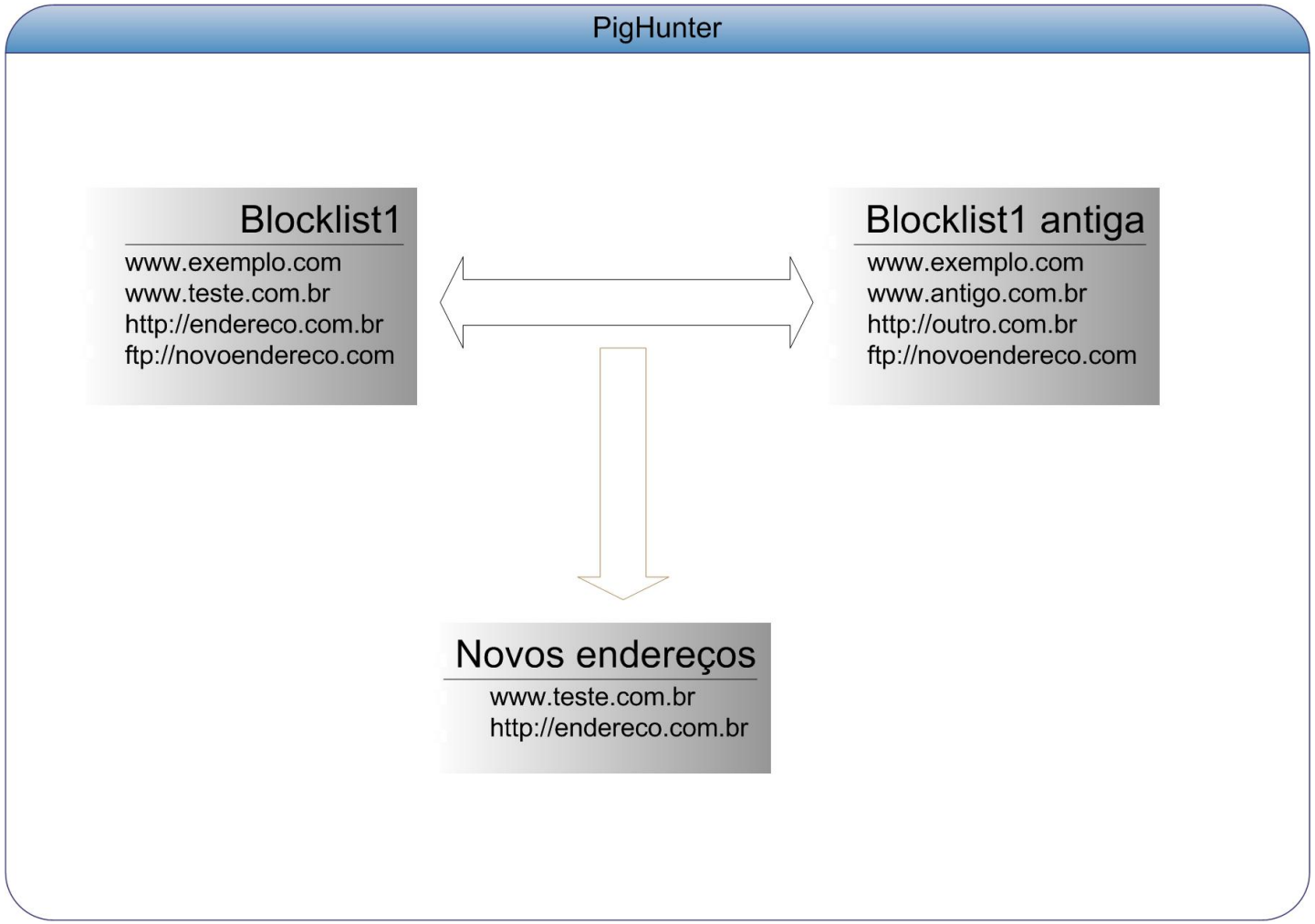
Via Blocklists



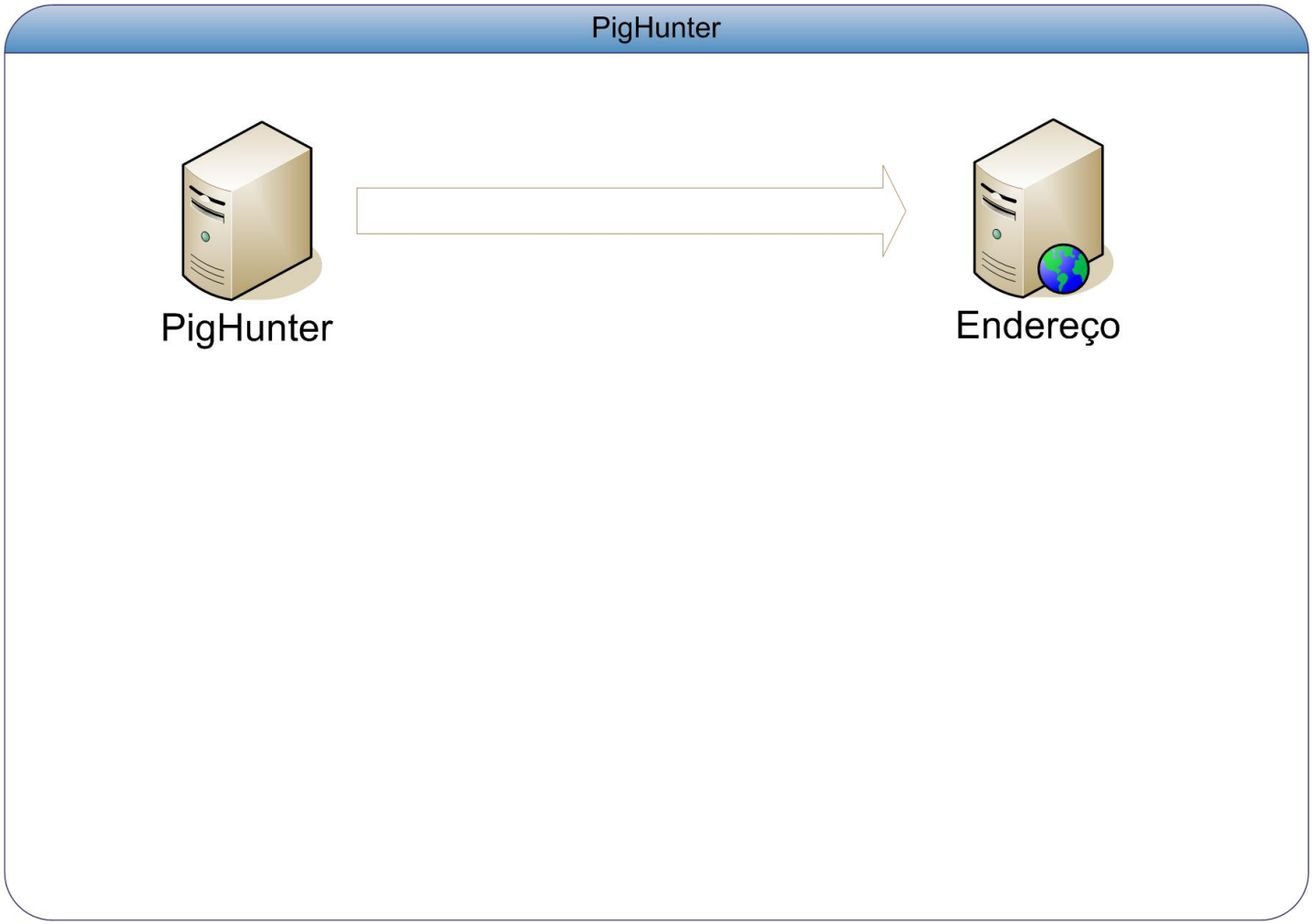
Via Blocklists



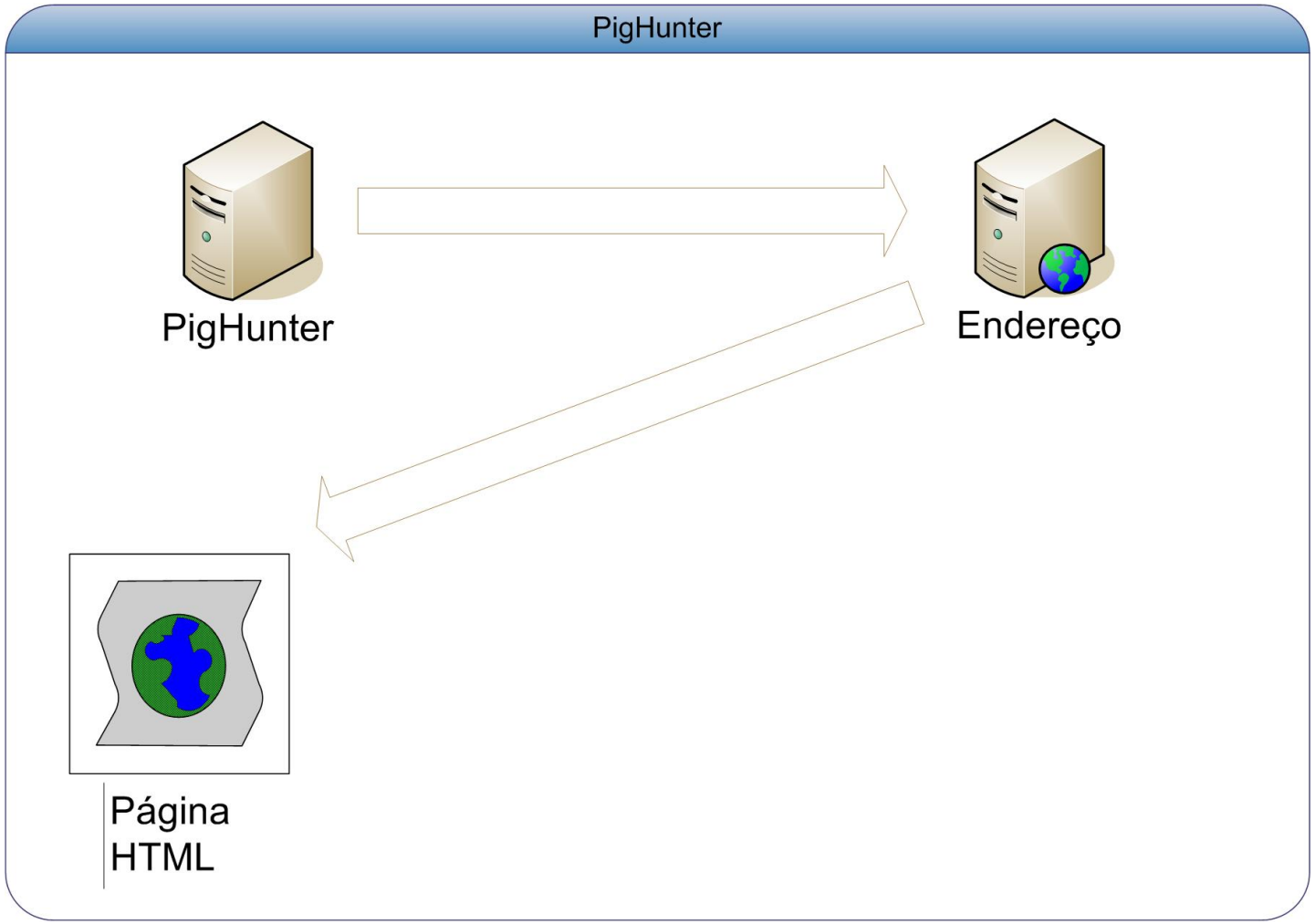
Via Blocklists



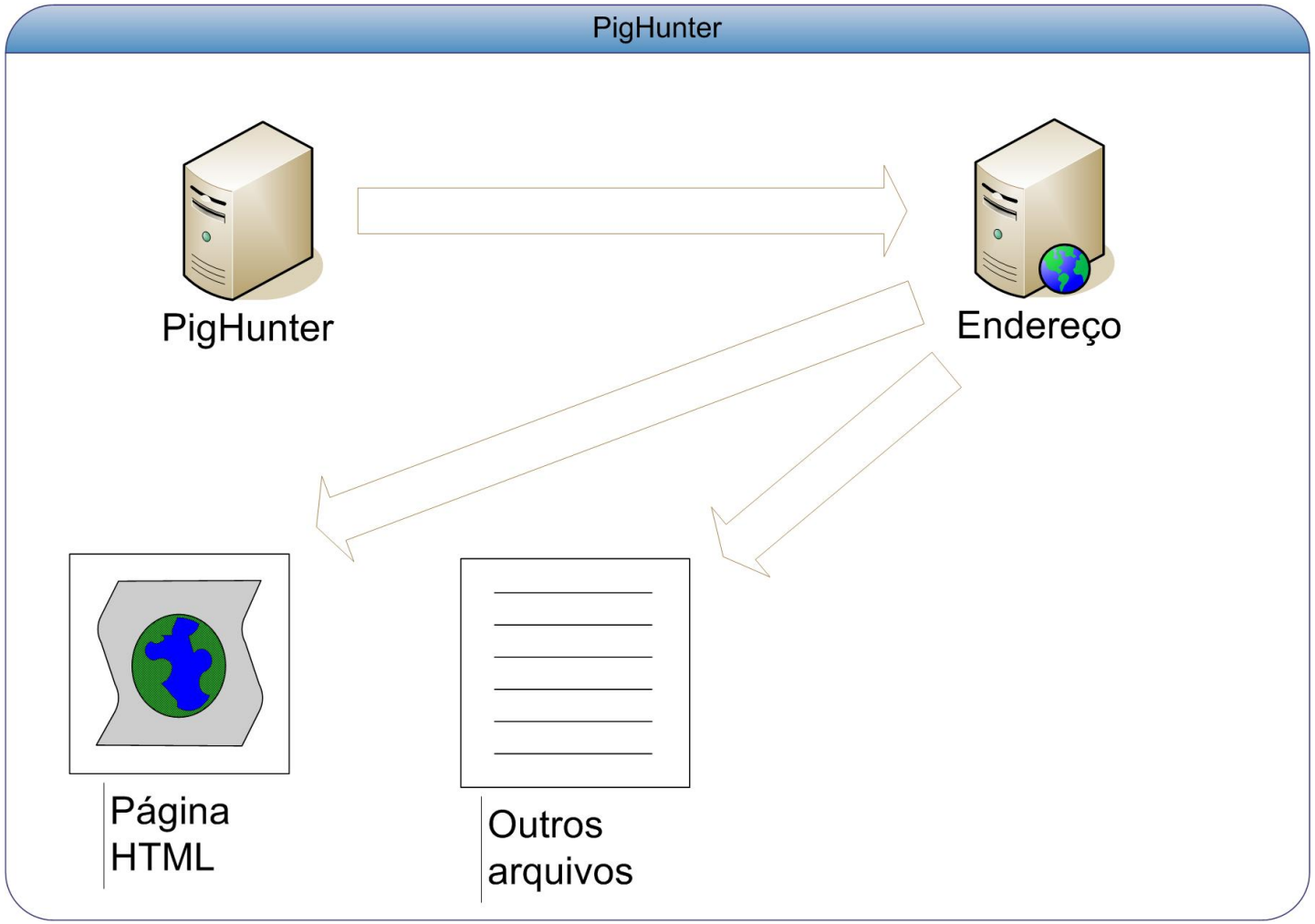
Processo de pesquisa em endereços



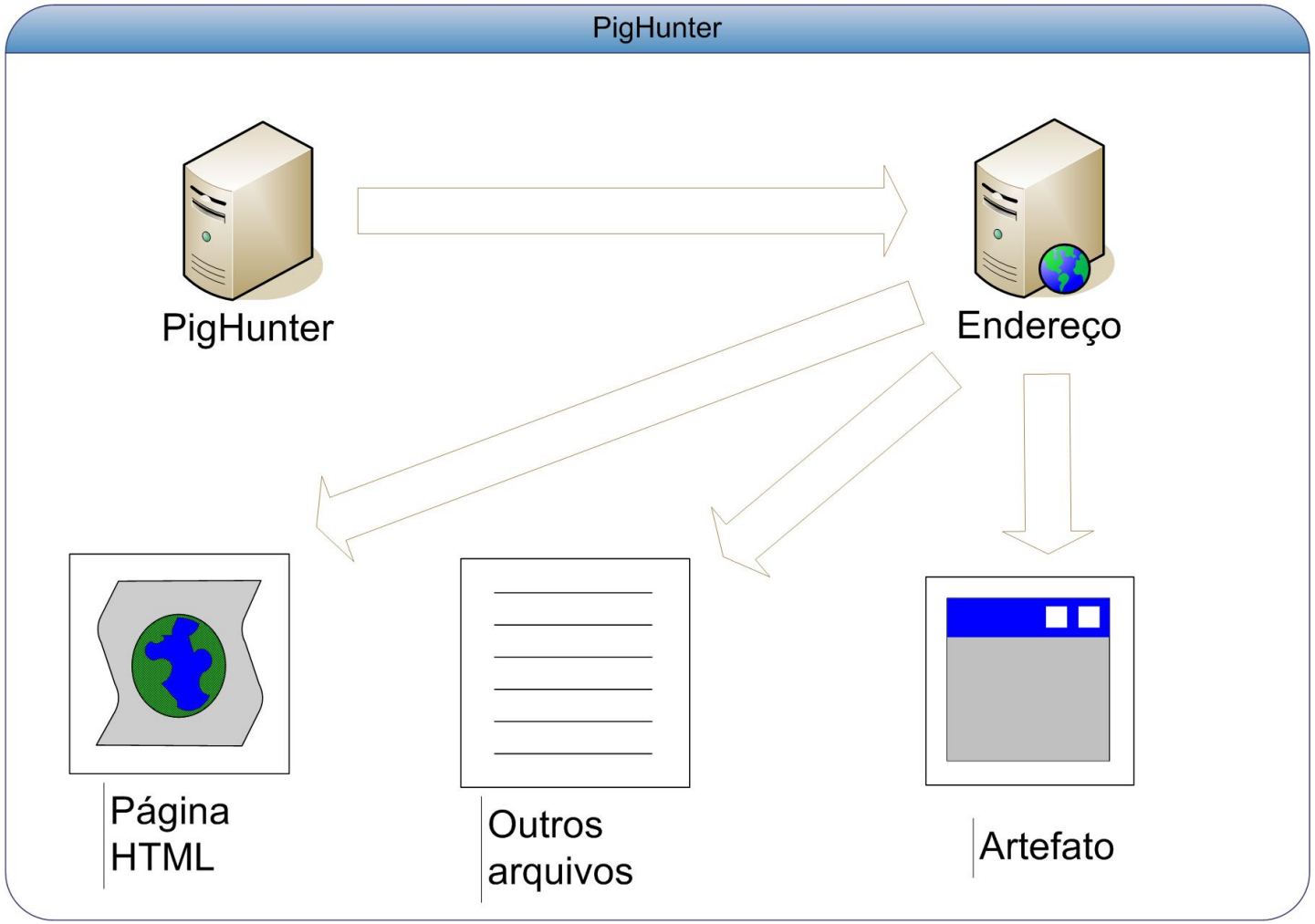
Processo de pesquisa em endereços



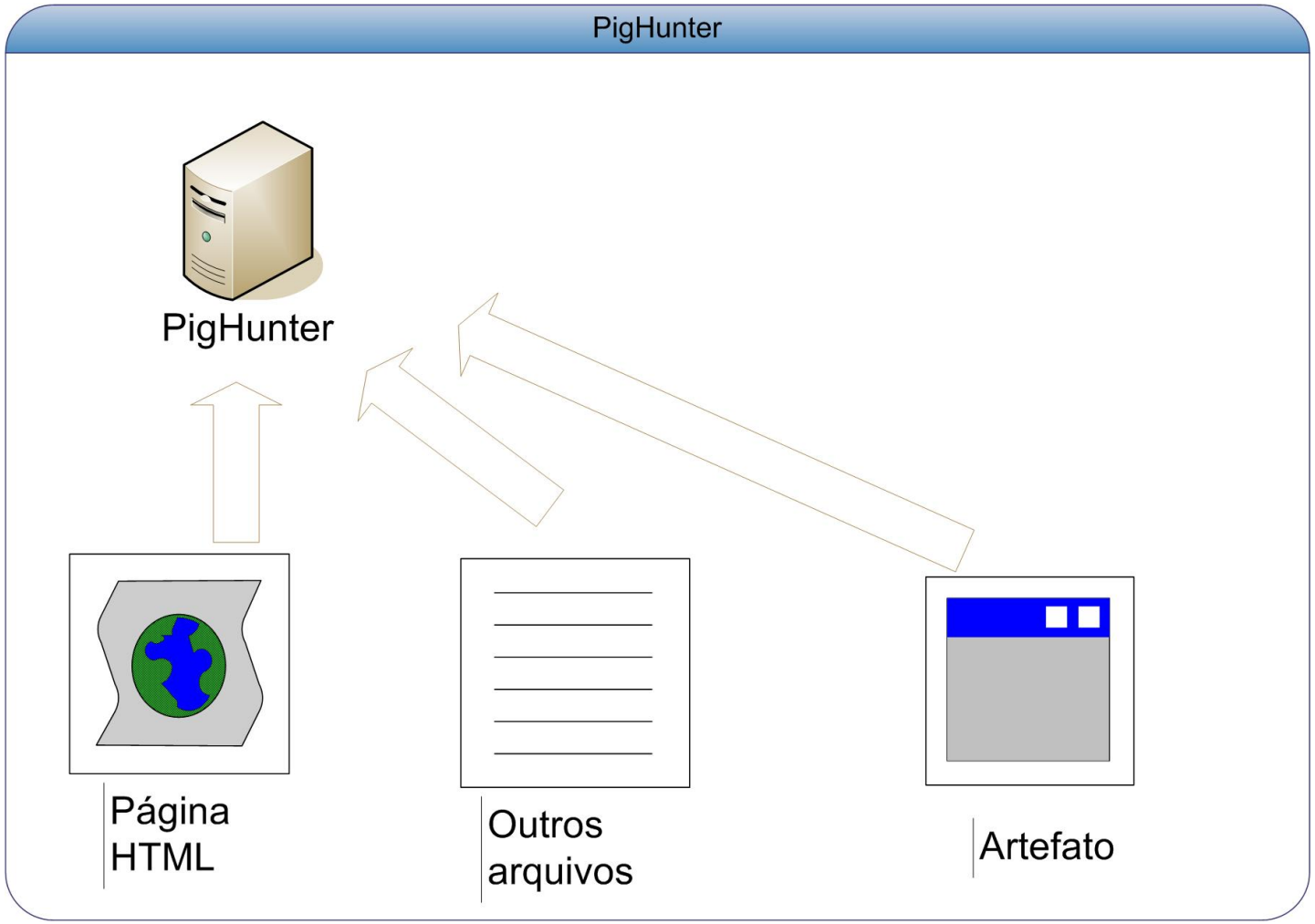
Processo de pesquisa em endereços



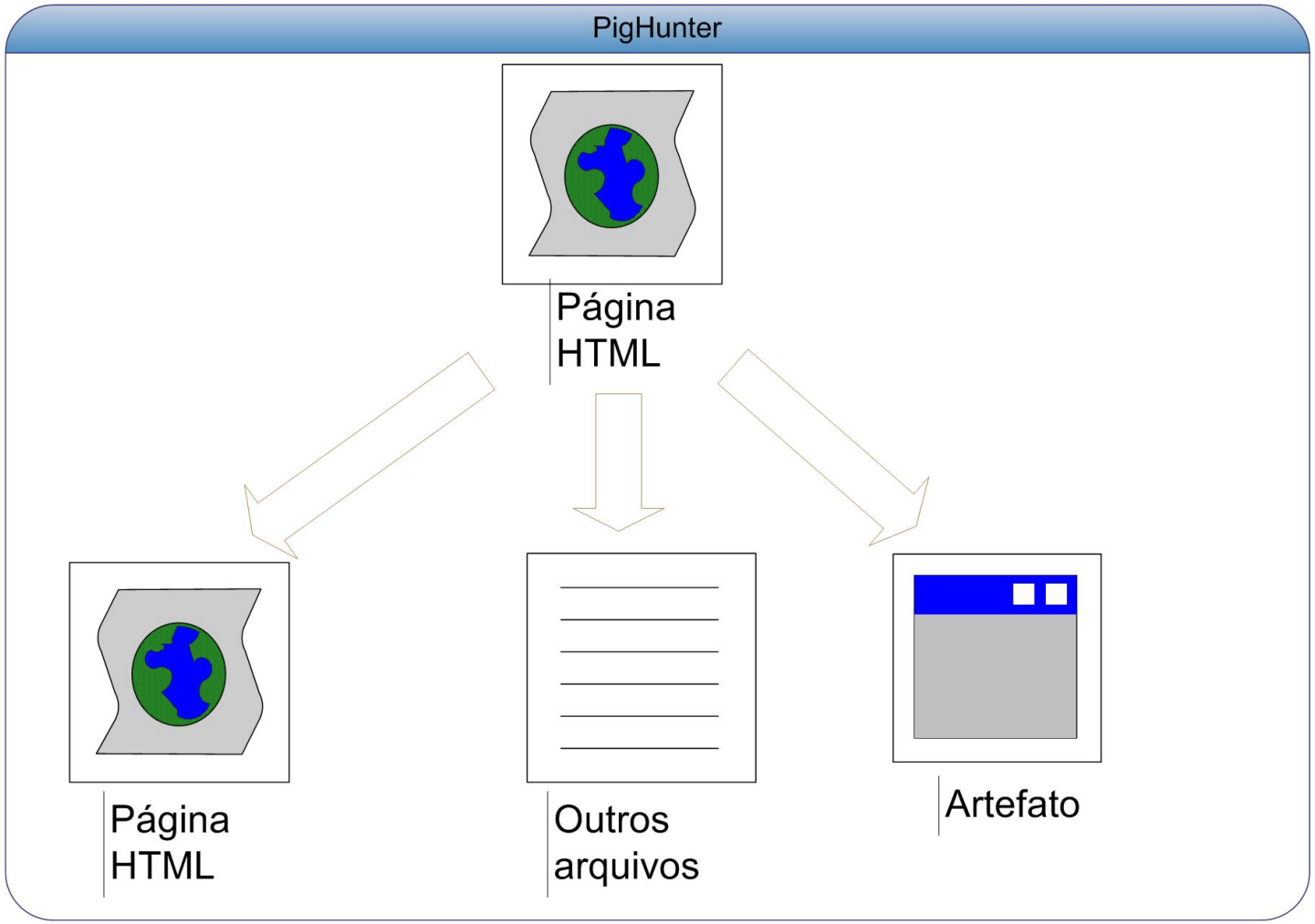
Processo de pesquisa em endereços



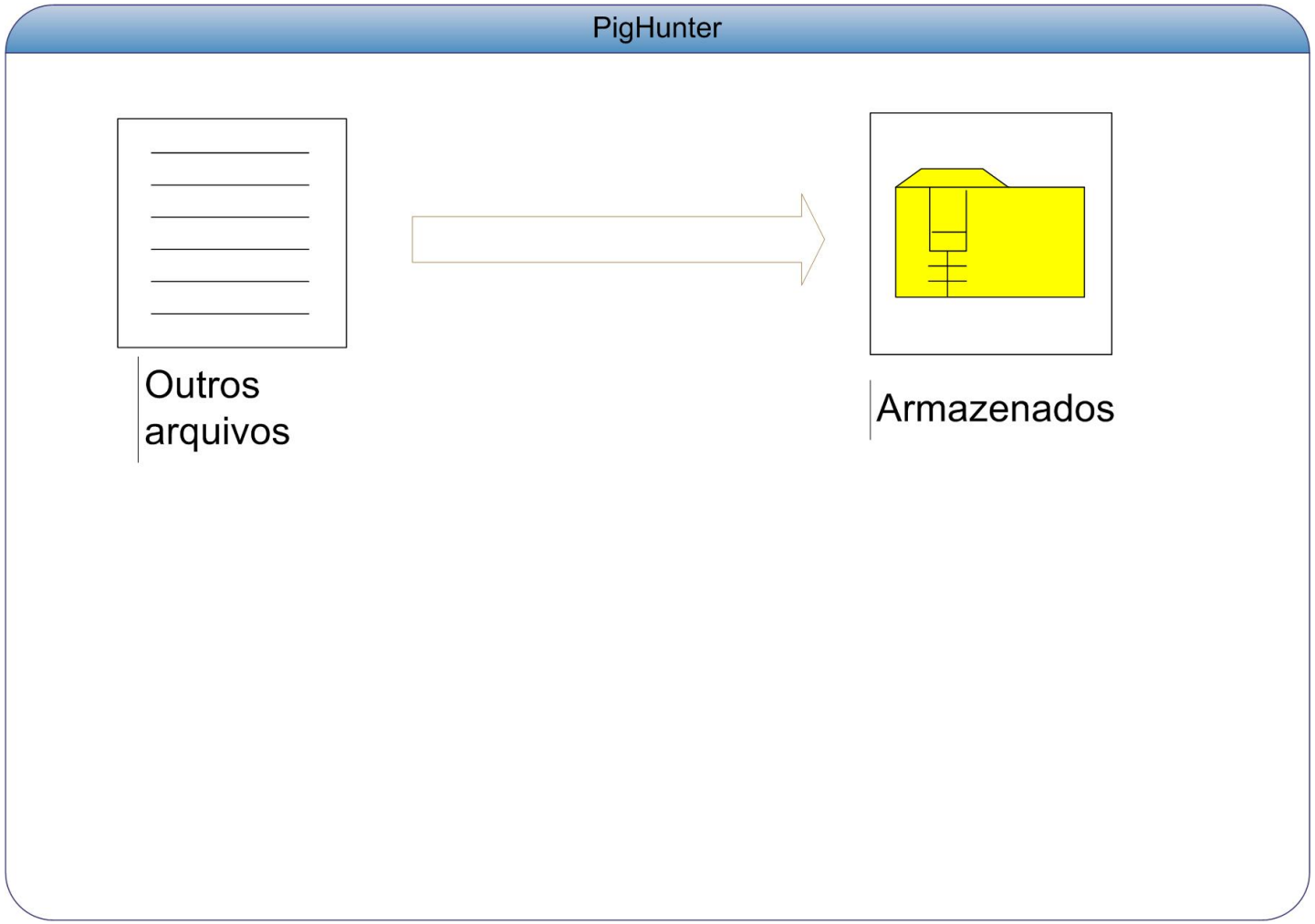
Processo de pesquisa em endereços



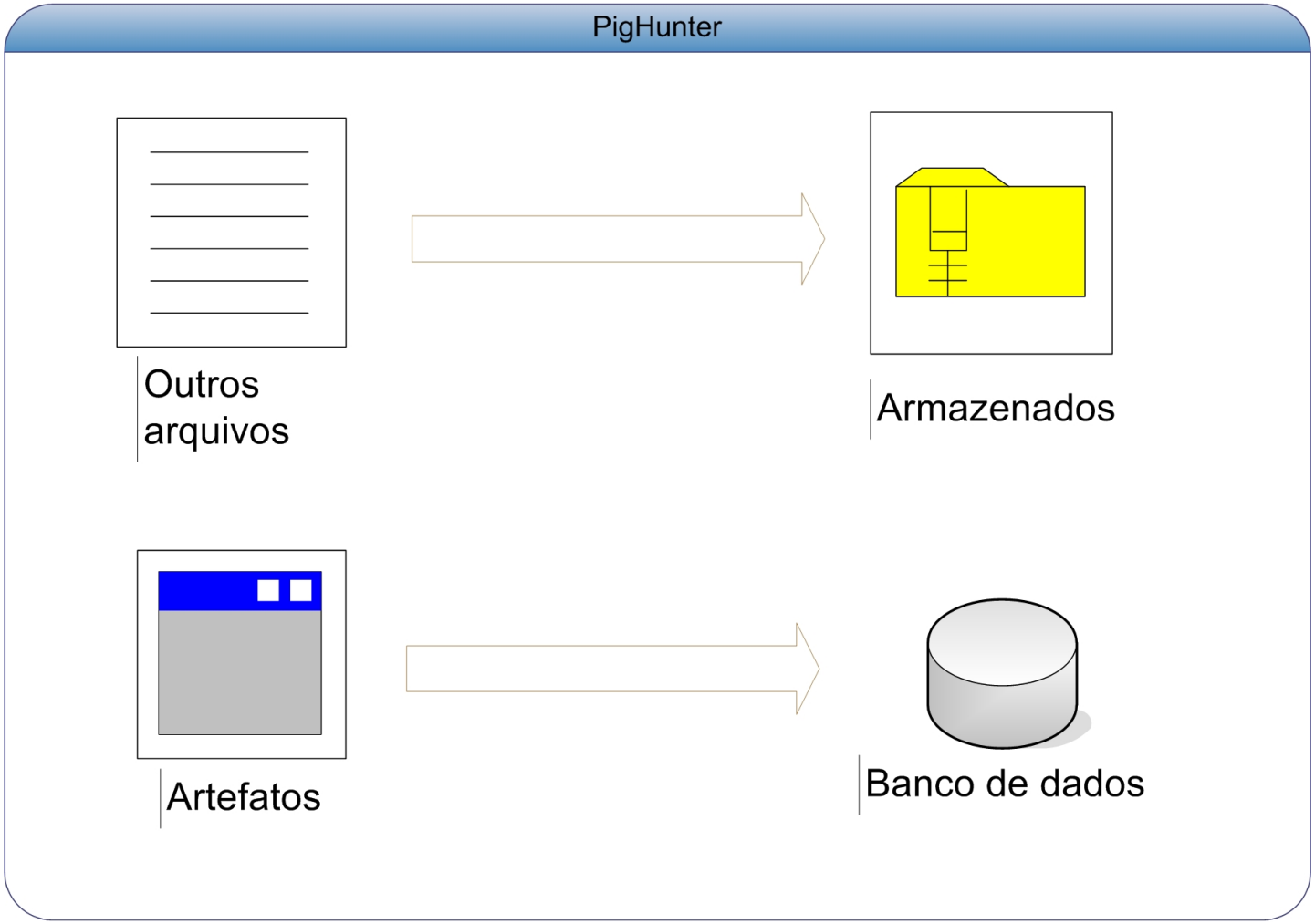
Processo de pesquisa em endereços



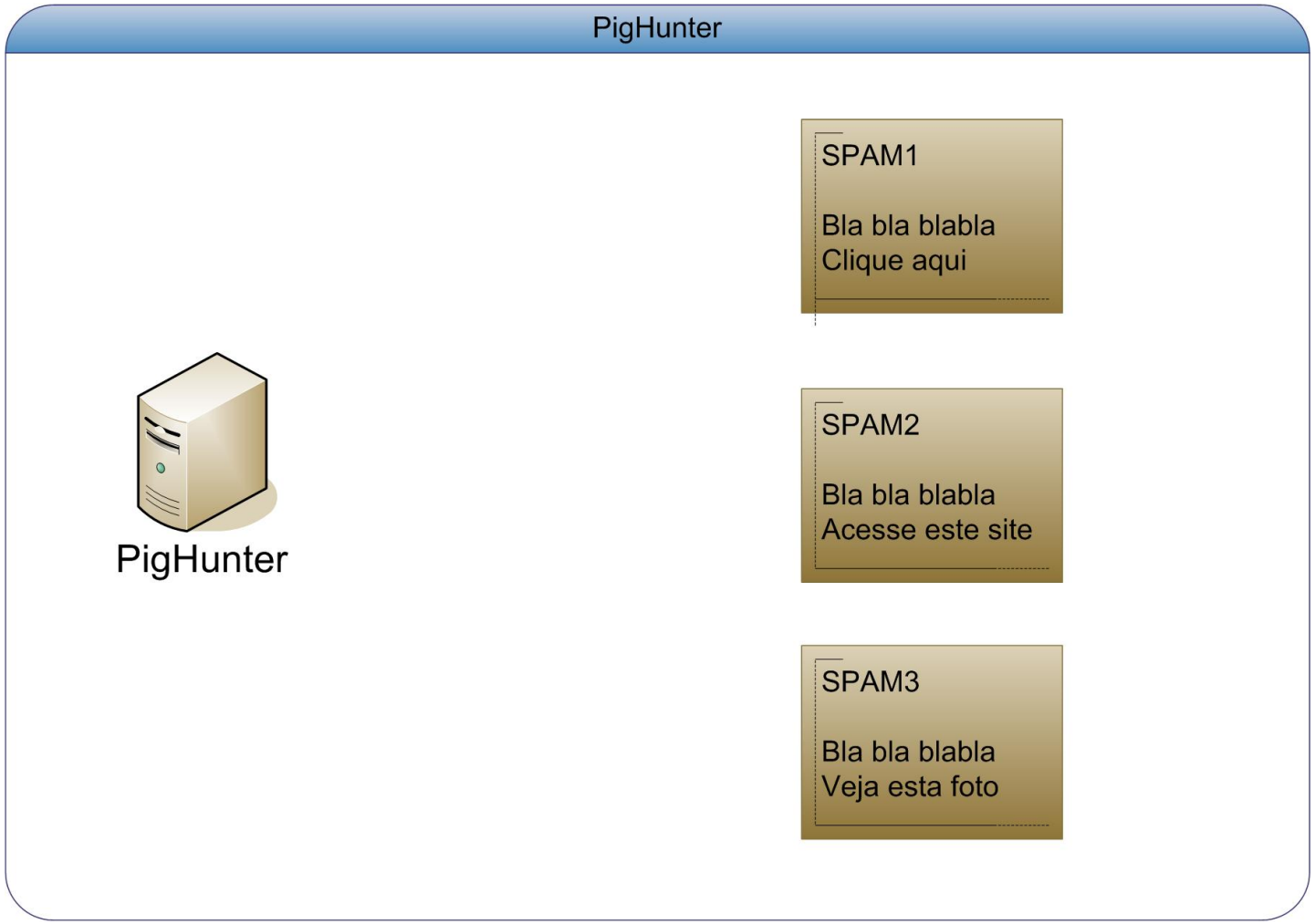
Processo de pesquisa em endereços



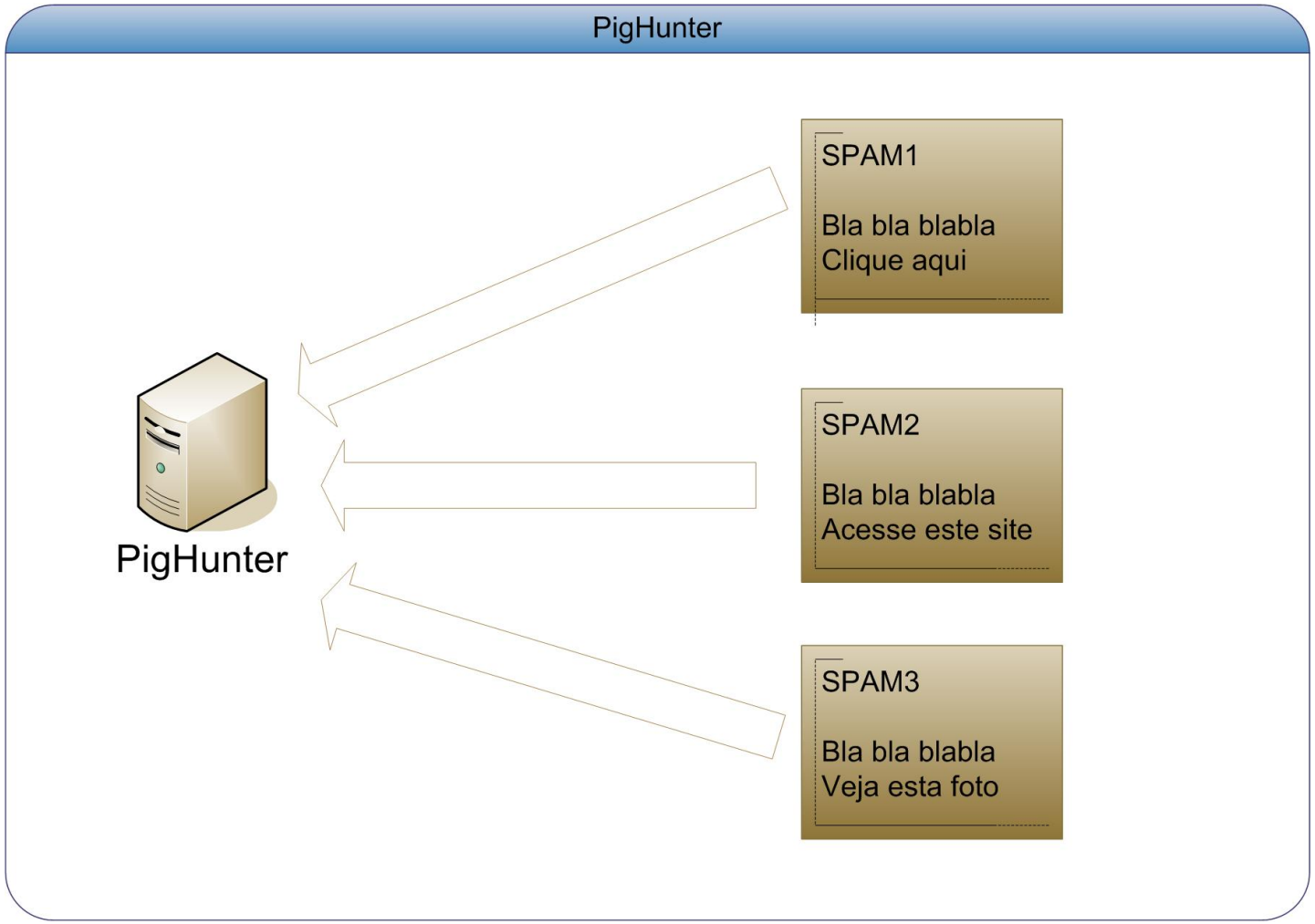
Processo de pesquisa em endereços



Via SPAMS


PigHunter
SPAM1
Bla bla blabla
Clique aqui
SPAM2
Bla bla blabla
Acesse este site
SPAM3
Bla bla blabla
Veja esta foto
PigHunter

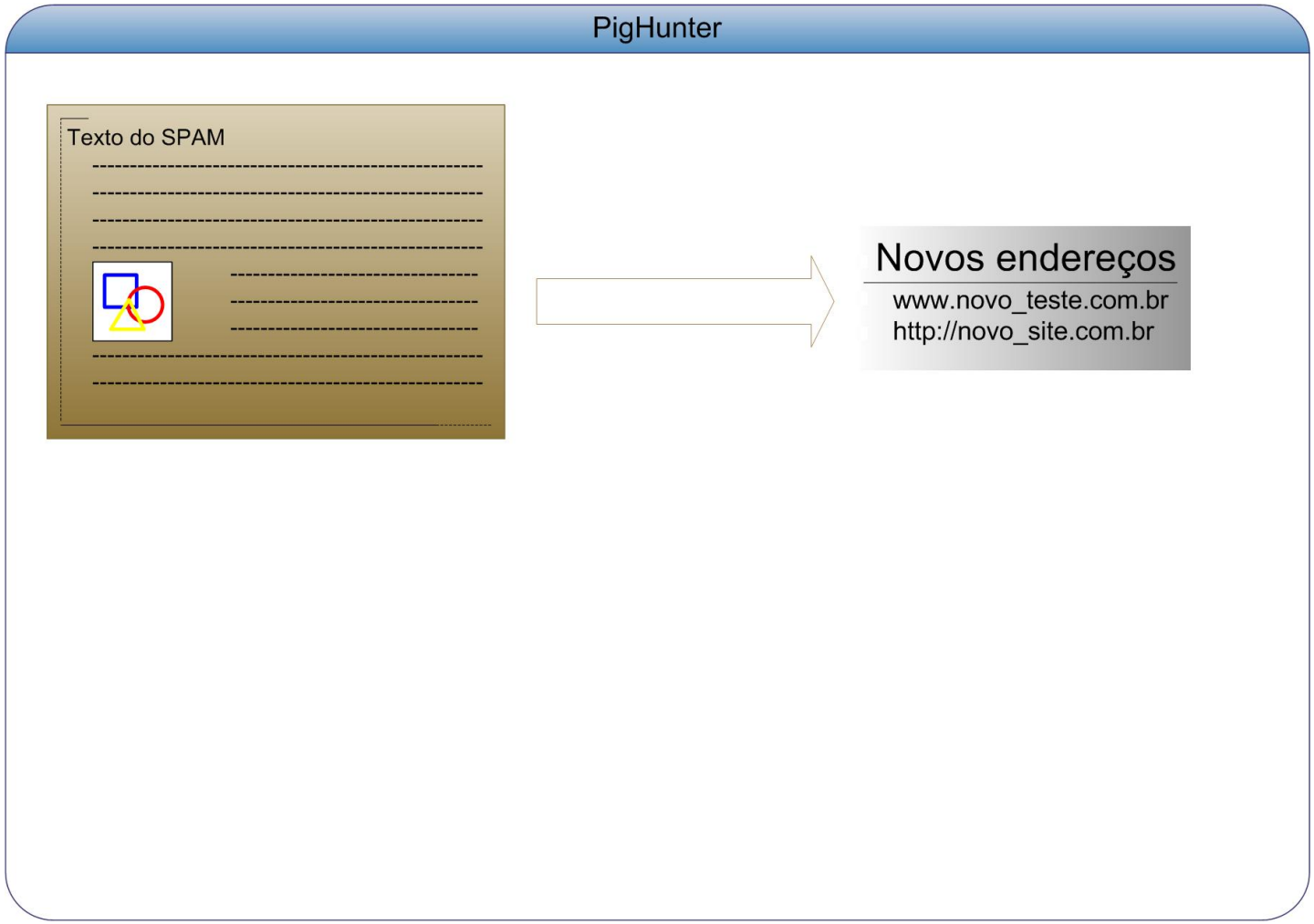
Via SPAMS


PigHunter
SPAM1
Bla bla blabla
Clique aqui
SPAM2
Bla bla blabla
Acesse este site
SPAM3
Bla bla blabla
Veja esta foto
PigHunter

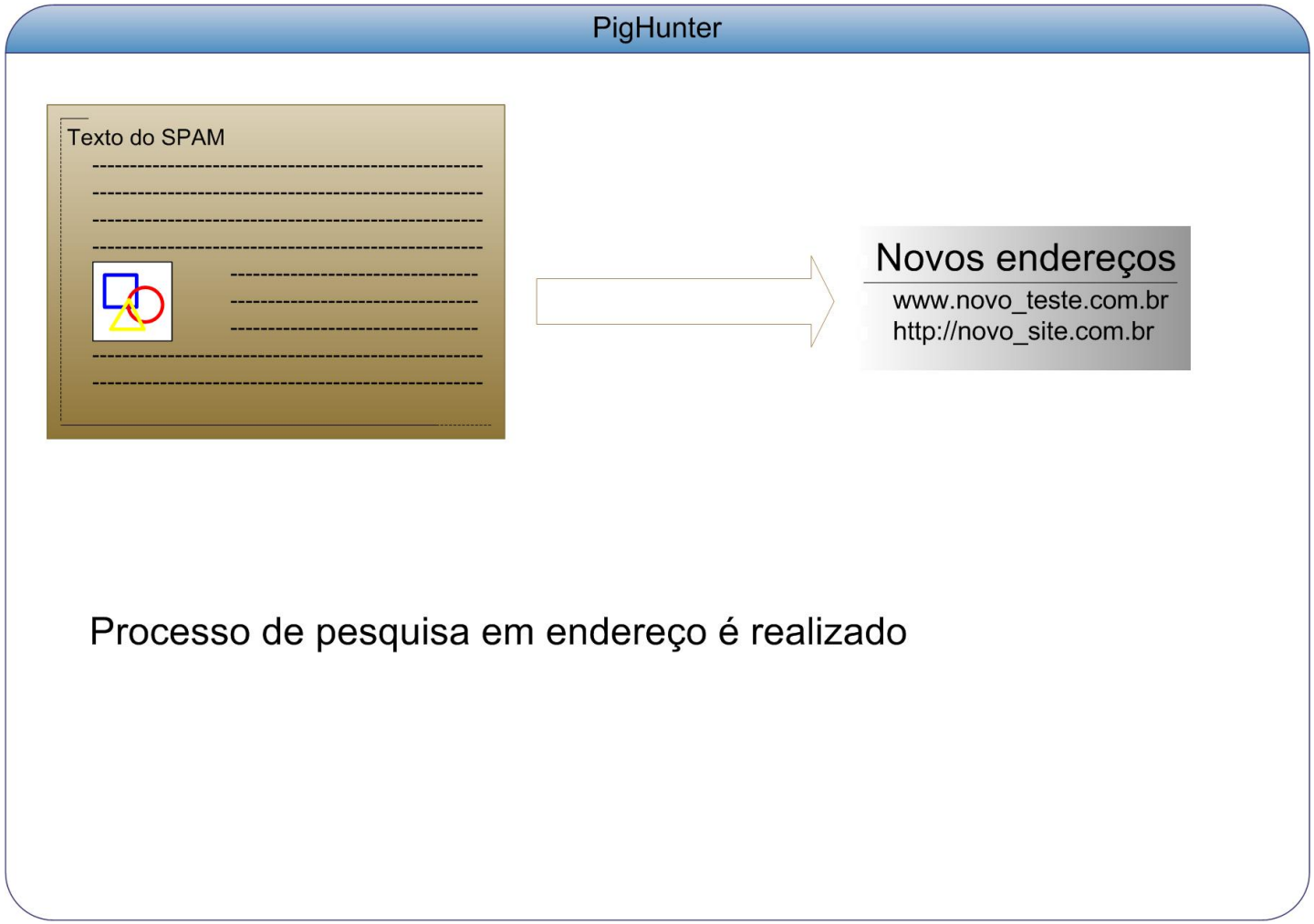
Via SPAMS

PigHunter

Via SPAMS


PigHunter
Texto do SPAM
Novos endereços
www.novo_teste.com.br
http://novo_site.com.br

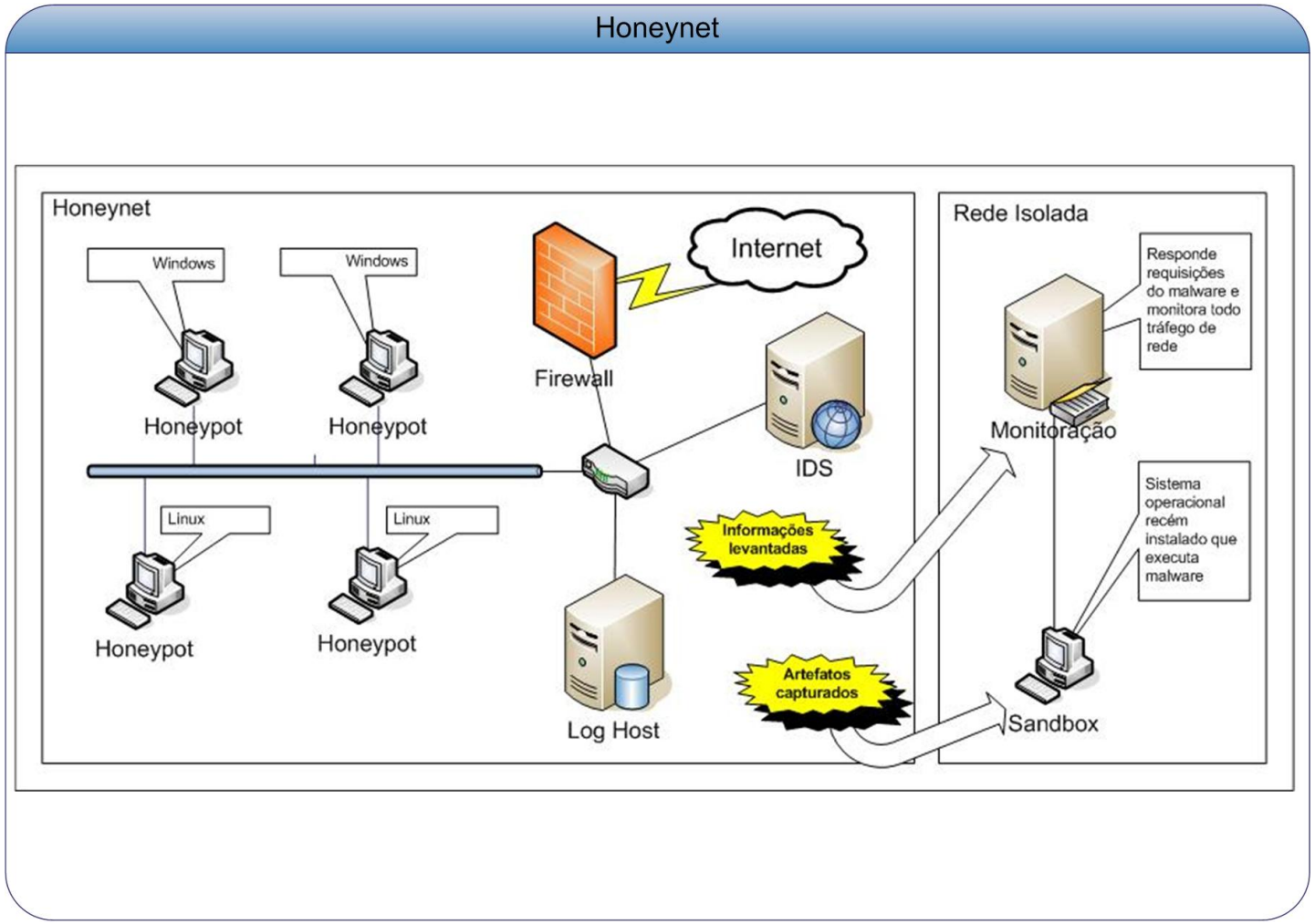
Via SPAMS


PigHunter
Texto do SPAM
Novos endereços
www.novo_teste.com.br
http://novo_site.com.br
Processo de pesquisa em endereço é realizado

Através da honeynet

- São coletados artefatos utilizados por atacantes da Honeynet
- Os artefatos ficam armazenados nas máquinas comprometidas pelos atacantes
- O Honeypot comprometido é analisado e o resultado pode auxiliar a análise do artefato

Através da honeynet



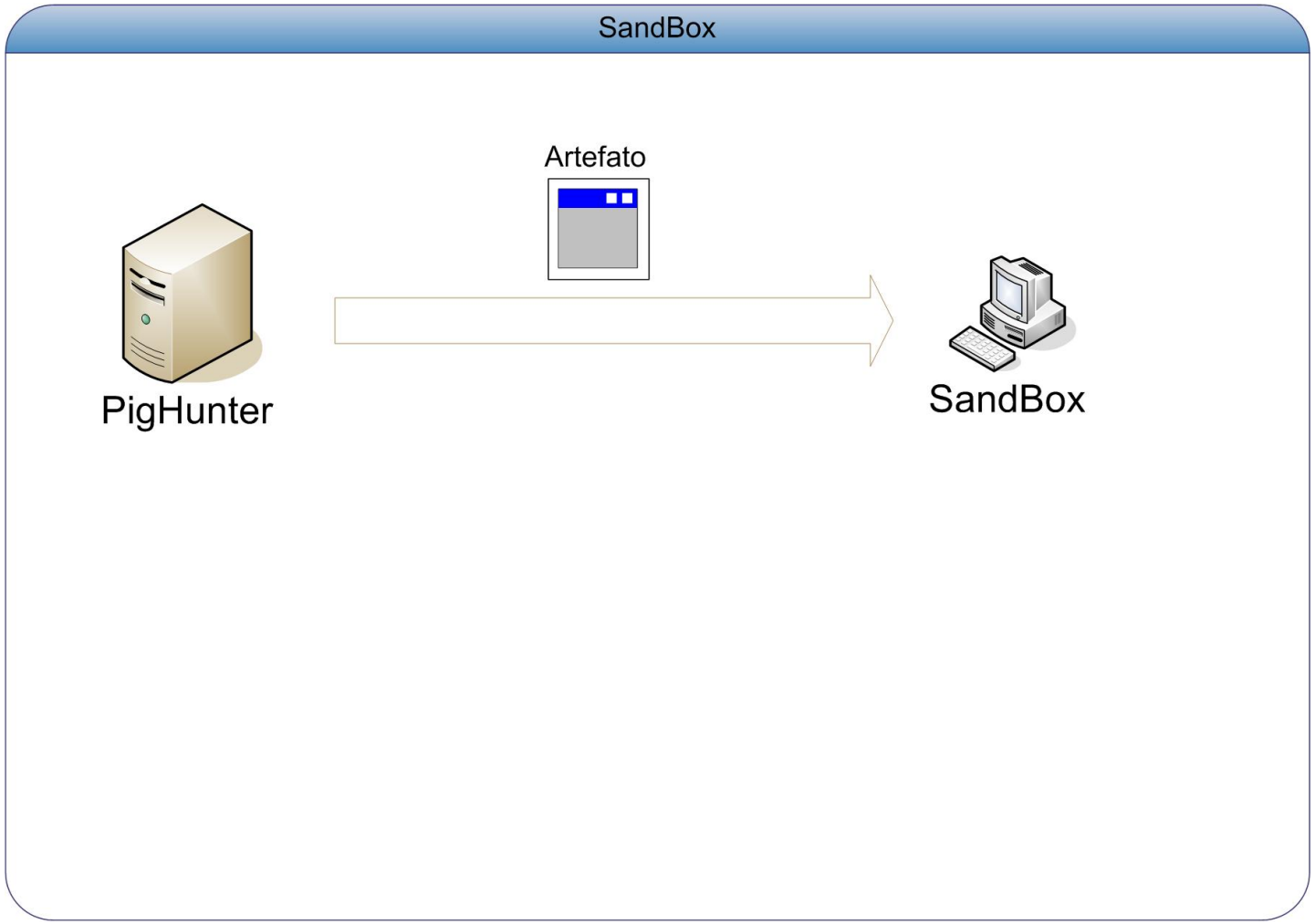
Índice

Pré-análise

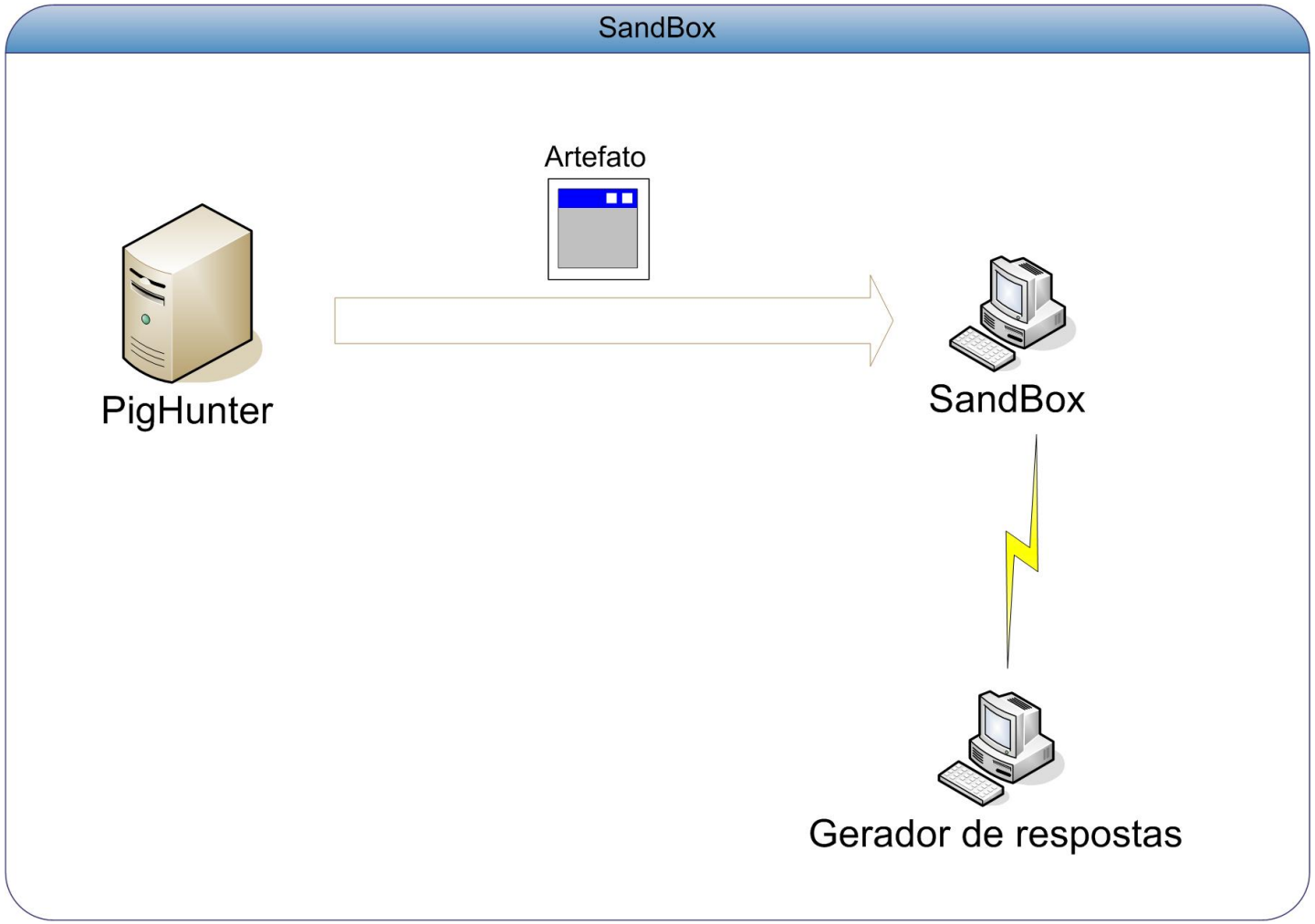
Realizada assim que o artefato é coletado
Informações coletadas:

- Tipo de artefato
- Hash
- Strings encontradas no código binário do artefato
- Packer utilizado
- DLL's que o artefato precisa para executar

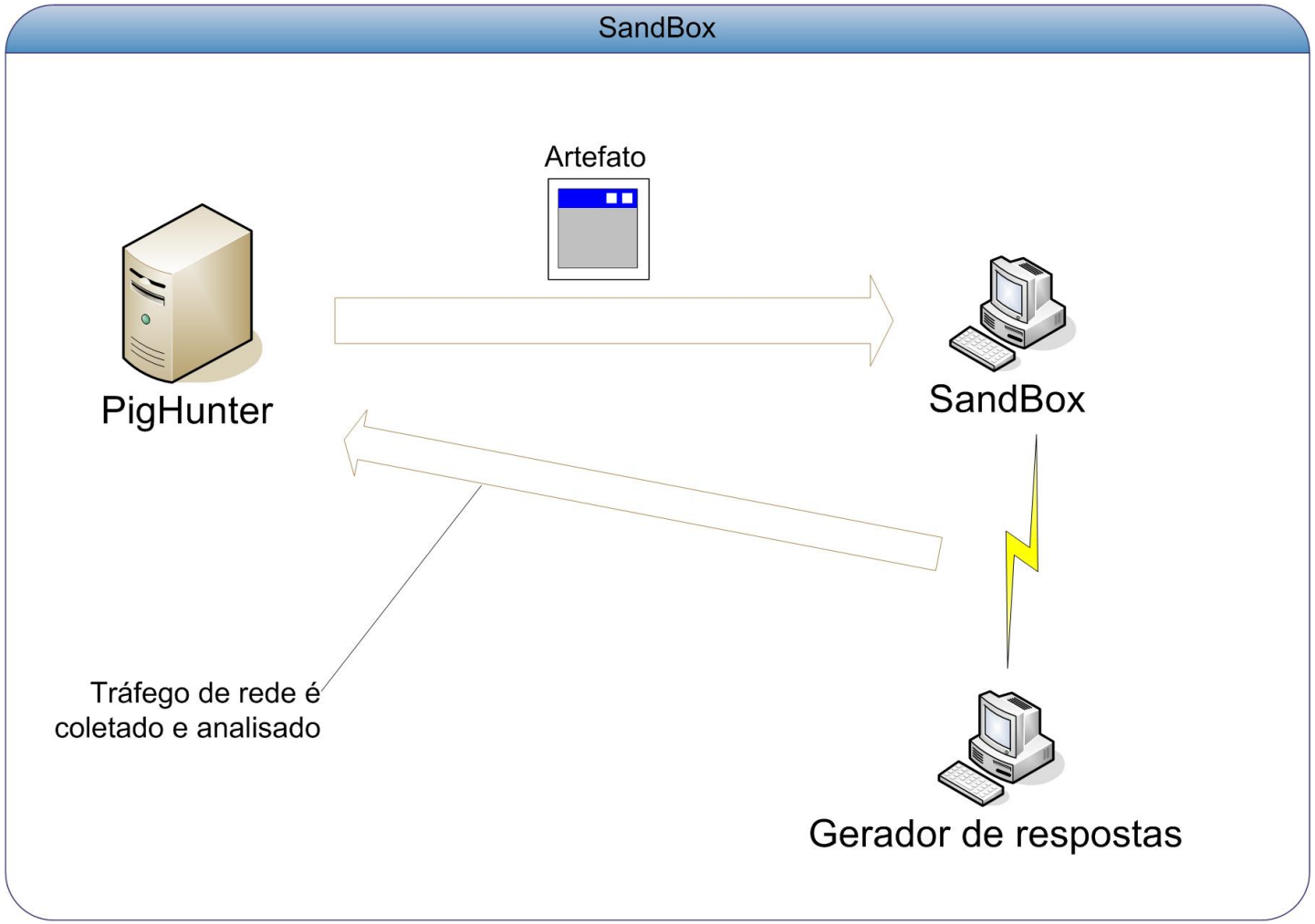
SandBox



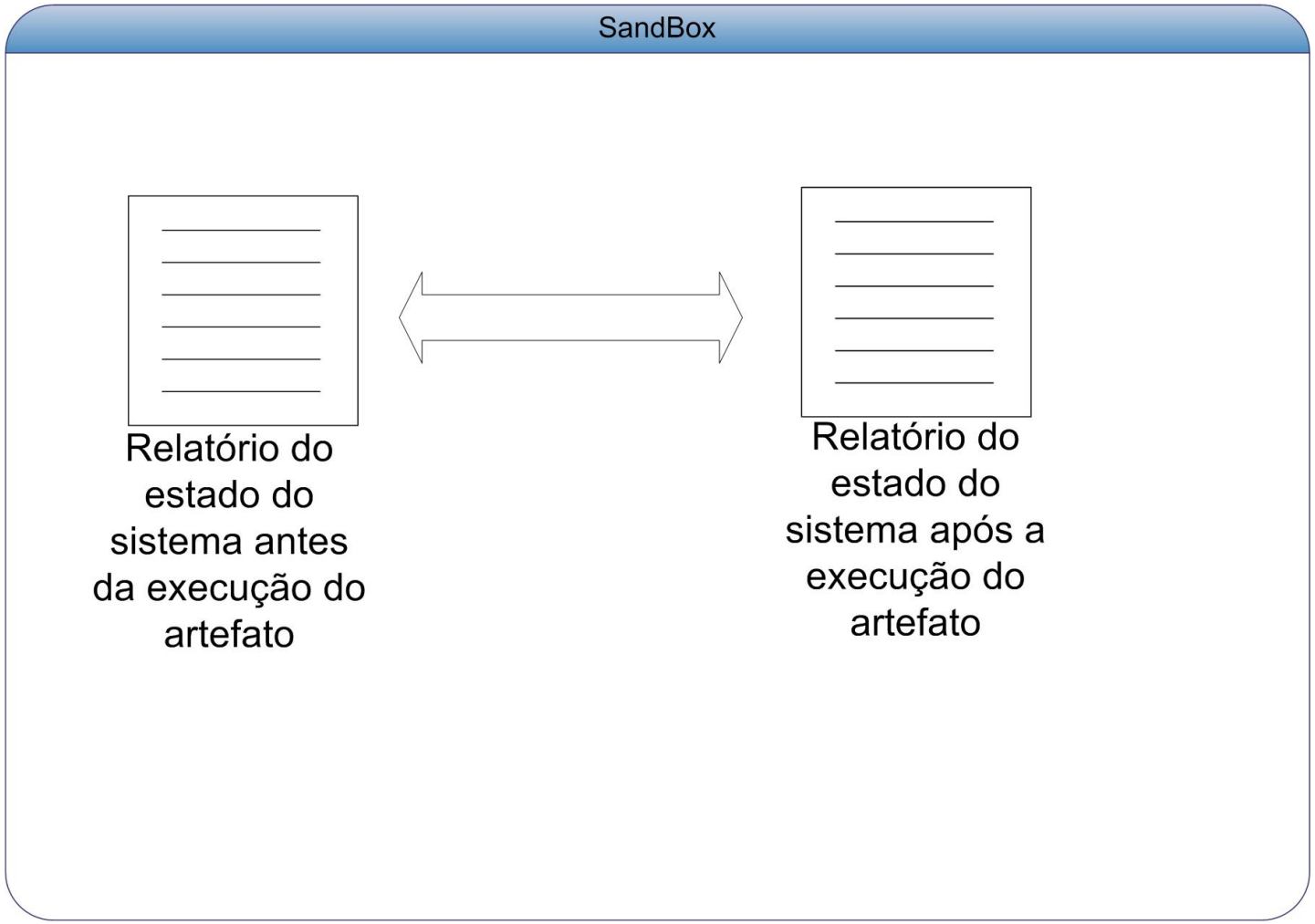
SandBox



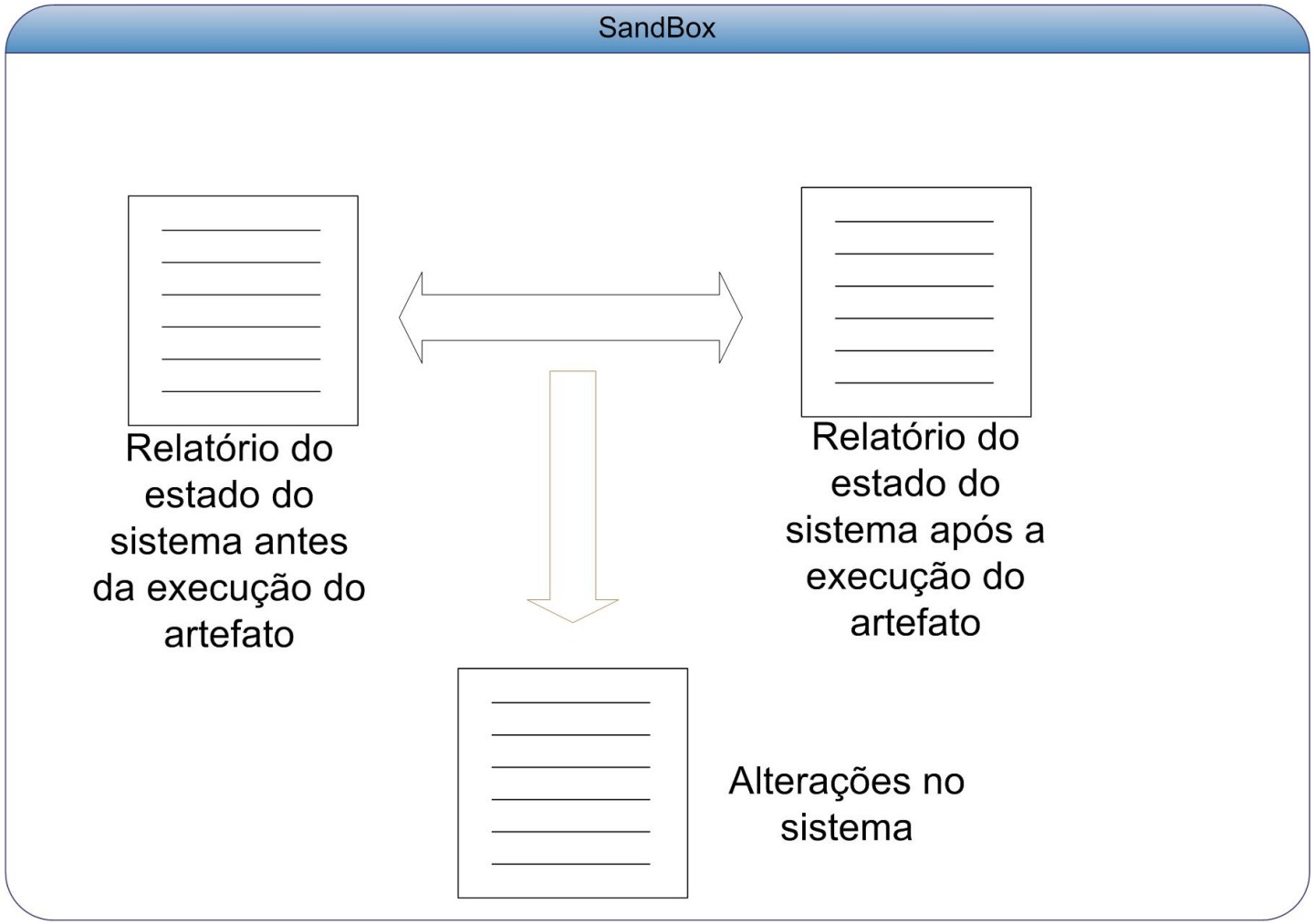
SandBox


SandBox
Artefato
PigHunter
SandBox
Tráfego de rede é
coletado e analisado
Gerador de respostas

SandBox


SandBox
Relatório do estado do sistema antes da execução do artefato
Relatório do estado do sistema após a execução do artefato

SandBox


SandBox
Relatório do estado do sistema antes da execução do artefato
Relatório do estado do sistema após a execução do artefato
Alterações no sistema

SandBox

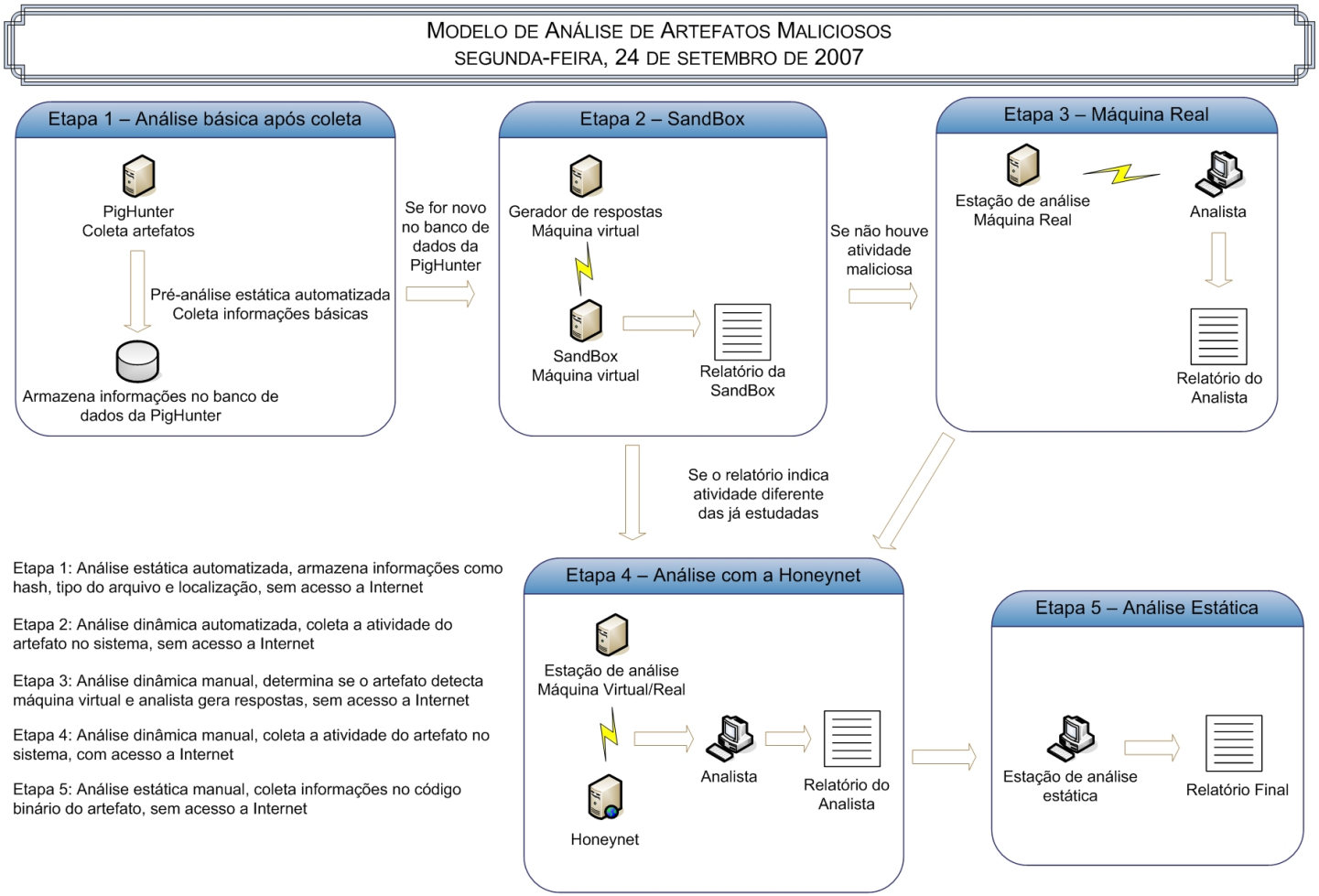
Informações coletadas:

- Tráfego de rede
- Arquivos adicionados, alterados ou excluídos do sistema
- Registro do sistema
- Programas que entraram em execução
- Portas abertas
- Programas configurados para inicializar com o sistema

Análise utilizando Honeynet

- Os artefatos que precisam de saída para a Internet, são colocados em execução na Honeynet
- Como o tráfego de saída da Honeynet é controlado, o artefato não poderá causar danos em máquinas fora da Honeynet
- Os resultados obtidos com a utilização da Honeynet na análise foram satisfatórios

Modelo de análise



Índice

Tipos de artefatos maliciosos

- Trojan horse: Abre uma porta (backdoor) para manipulação remota da máquina
- Boot: Vírus que se infecta na área de inicialização dos discos rígidos
- Botclient: Se conecta a um canal de comunicação aguardando instruções

Tipos de artefatos maliciosos

- Trojan horse: Abre uma porta (backdoor) para manipulação remota da máquina
- Boot: Vírus que se infecta na área de inicialização dos discos rígidos
- Botclient: Se conecta a um canal de comunicação aguardando instruções

Tipos de artefatos maliciosos

- Trojan horse: Abre uma porta (backdoor) para manipulação remota da máquina
- Boot: Vírus que se infecta na área de inicialização dos discos rígidos
- Botclient: Se conecta a um canal de comunicação aguardando instruções

Tipos de artefatos maliciosos

- Spyware: Envia informações do computador infectado para outro computador
- Keylogger: Captura as teclas digitadas no computador
- Worms: Se espalham através da rede utilizando pastas compartilhadas e falhas de segurança
- Rootkit: Permite que o atacante tenha privilégios de administrador do computador

Tipos de artefatos maliciosos

- Spyware: Envia informações do computador infectado para outro computador
- Keylogger: Captura as teclas digitadas no computador
- Worms: Se espalham através da rede utilizando pastas compartilhadas e falhas de segurança
- Rootkit: Permite que o atacante tenha privilégios de administrador do computador

Tipos de artefatos maliciosos

- Spyware: Envia informações do computador infectado para outro computador
- Keylogger: Captura as teclas digitadas no computador
- Worms: Se espalham através da rede utilizando pastas compartilhadas e falhas de segurança
- Rootkit: Permite que o atacante tenha privilégios de administrador do computador

Tipos de artefatos maliciosos

- Spyware: Envia informações do computador infectado para outro computador
- Keylogger: Captura as teclas digitadas no computador
- Worms: Se espalham através da rede utilizando pastas compartilhadas e falhas de segurança
- Rootkit: Permite que o atacante tenha privilégios de administrador do computador

Índice

Técnicas utilizadas pelos artefatos

- Detecção de máquina virtual
- Empacotamento do código binário
- Detecção do uso de depurador

Detecção de máquina virtual

- Problema: Alguns artefatos não realizavam nenhuma operação
- Motivo: Os artefatos detectavam que estavam em uma máquina virtual
- Porque: Supunham estar sobre análise e ocultavam seu funcionamento
- Solução: Alterar a parte do código que detecta a máquina virtual

Detecção de máquina virtual

- Problema: Alguns artefatos não realizavam nenhuma operação
- Motivo: Os artefatos detectavam que estavam em uma máquina virtual
- Porque: Supunham estar sobre análise e ocultavam seu funcionamento
- Solução: Alterar a parte do código que detecta a máquina virtual

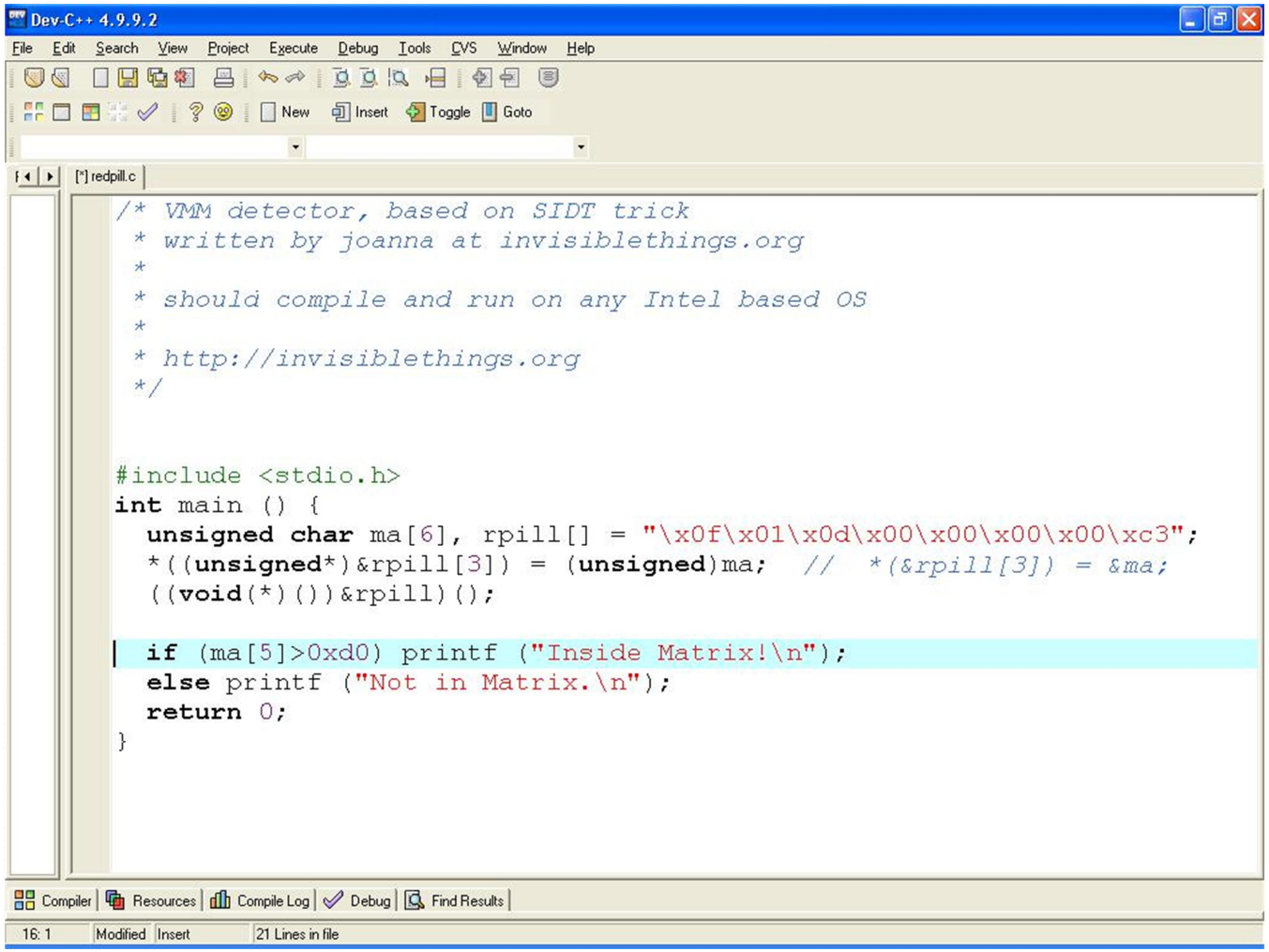
Detecção de máquina virtual

- Problema: Alguns artefatos não realizavam nenhuma operação
- Motivo: Os artefatos detectavam que estavam em uma máquina virtual
- Porque: Supunham estar sobre análise e ocultavam seu funcionamento
- Solução: Alterar a parte do código que detecta a máquina virtual

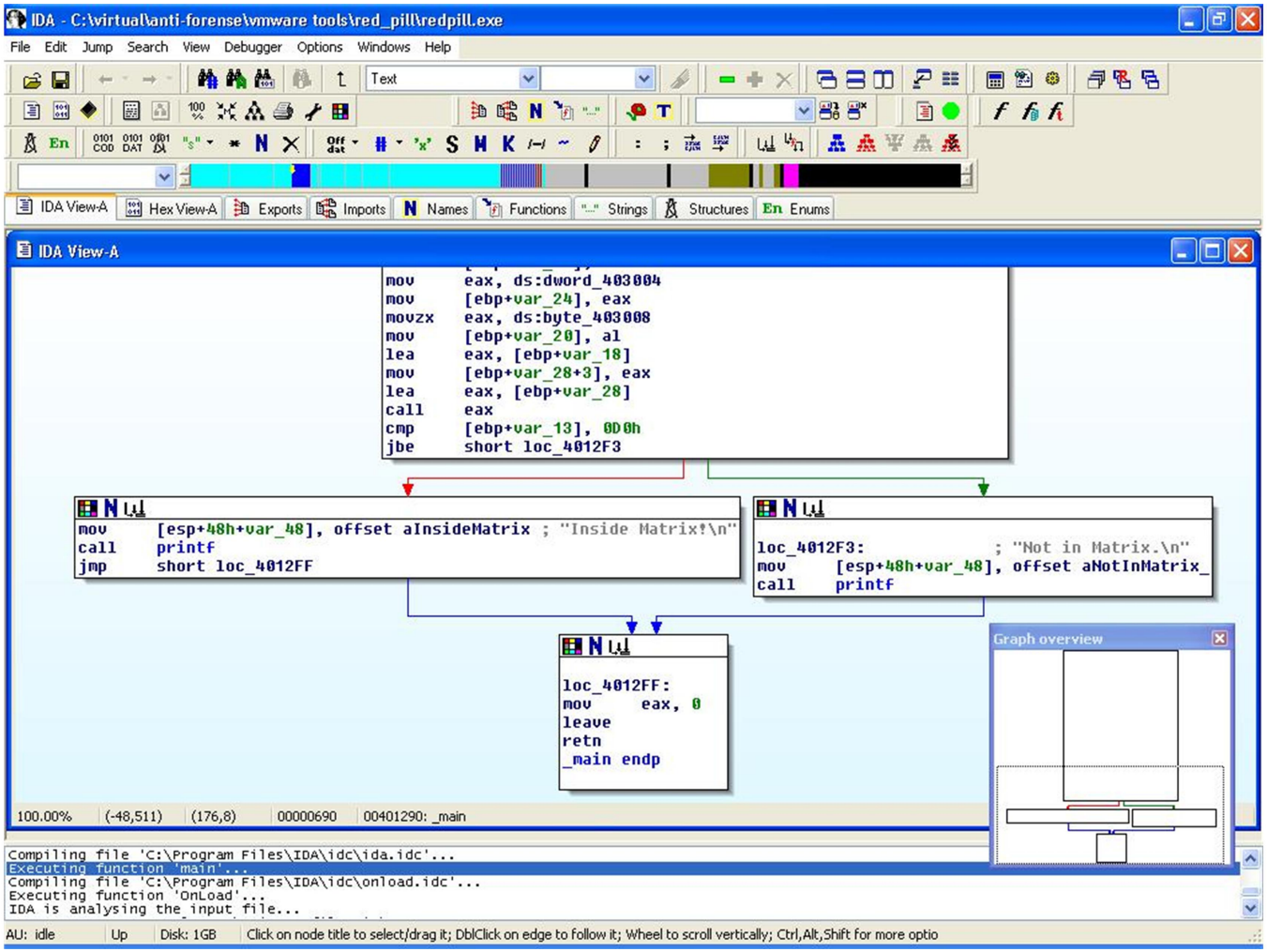
Detecção de máquina virtual

- Problema: Alguns artefatos não realizavam nenhuma operação
- Motivo: Os artefatos detectavam que estavam em uma máquina virtual
- Porque: Supunham estar sobre análise e ocultavam seu funcionamento
- Solução: Alterar a parte do código que detecta a máquina virtual

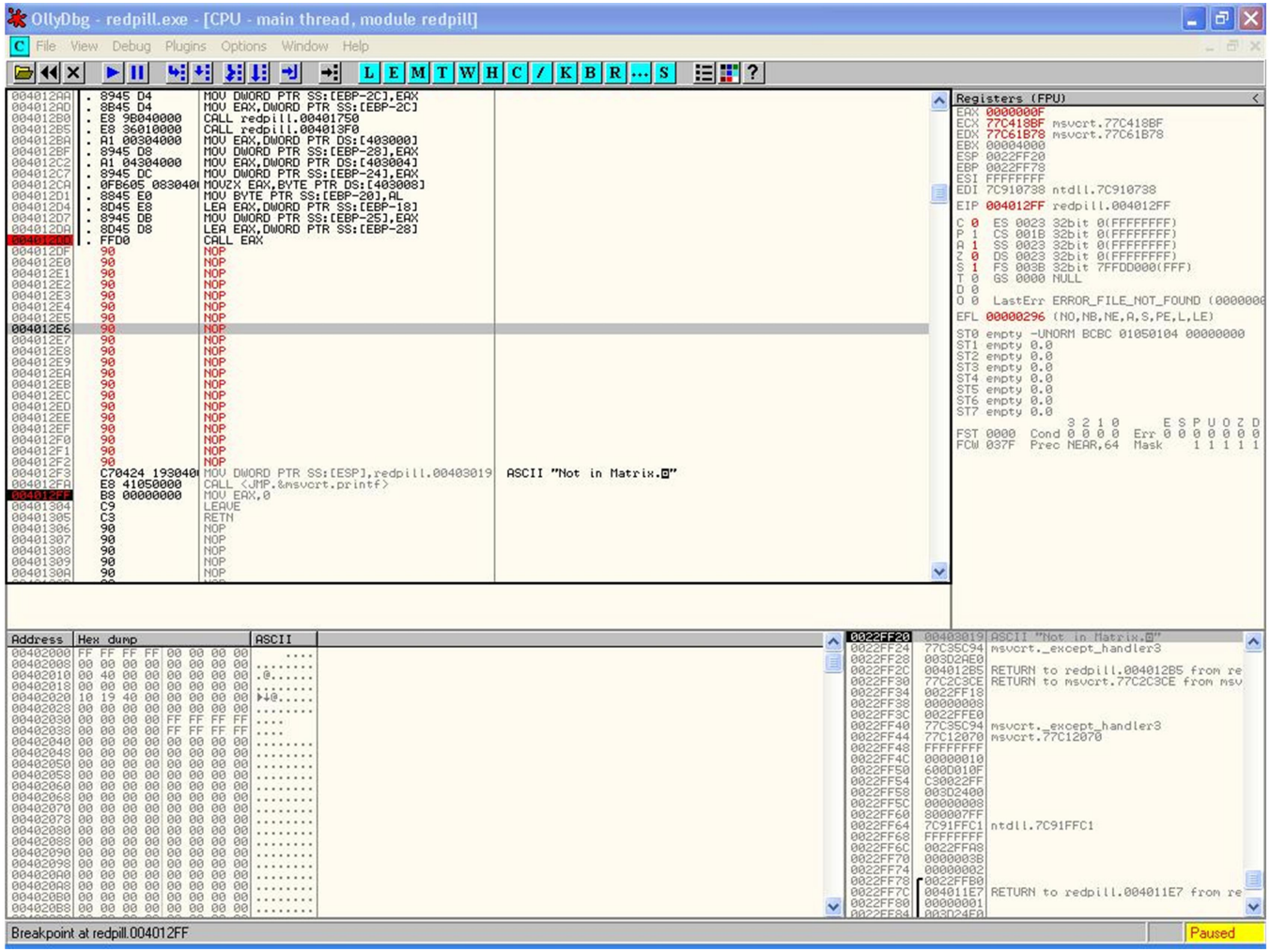
Detecção de máquina virtual



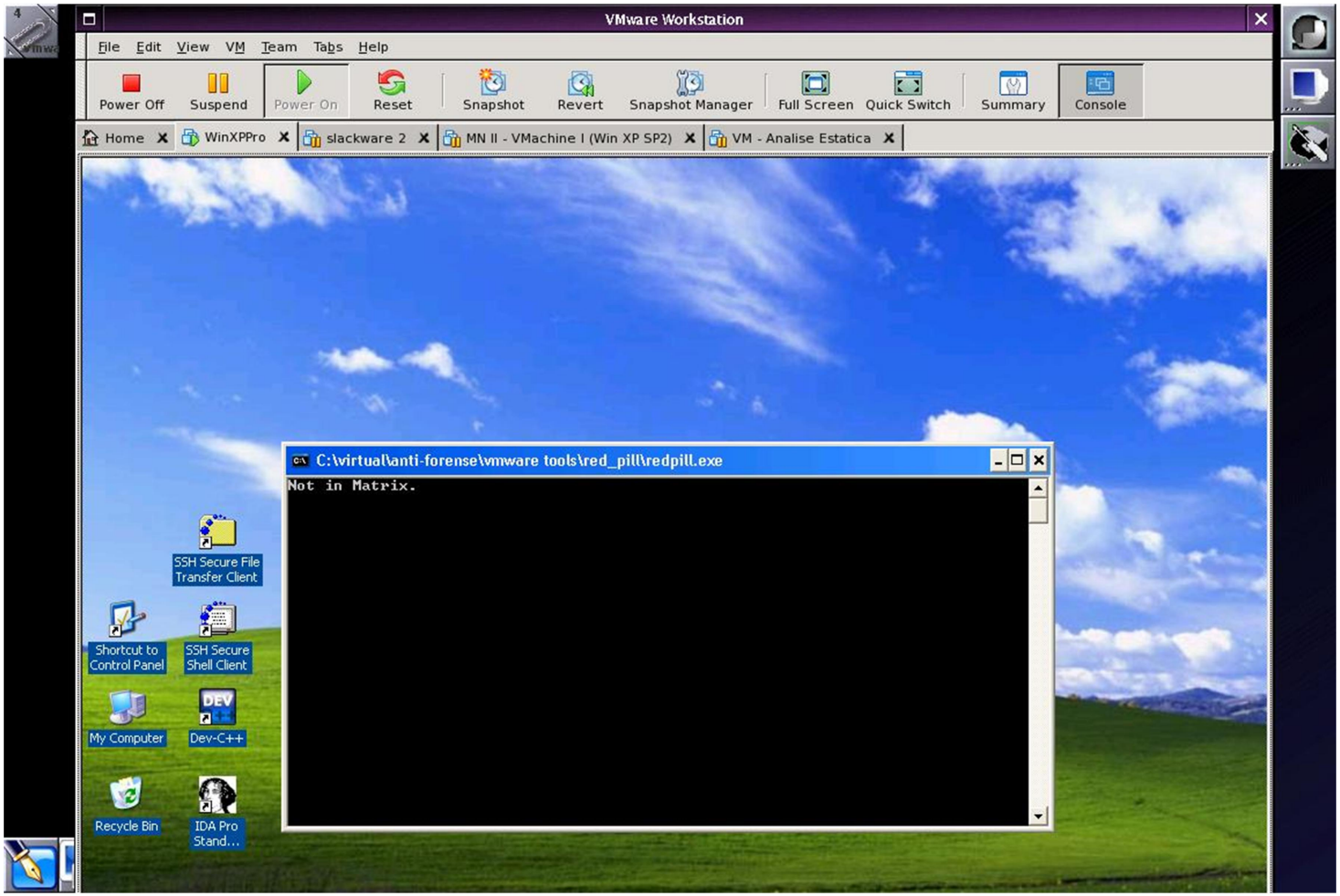
Detecção de máquina virtual



Detecção de máquina virtual



Detecção de máquina virtual



Empacotamento do código binário

Funções:

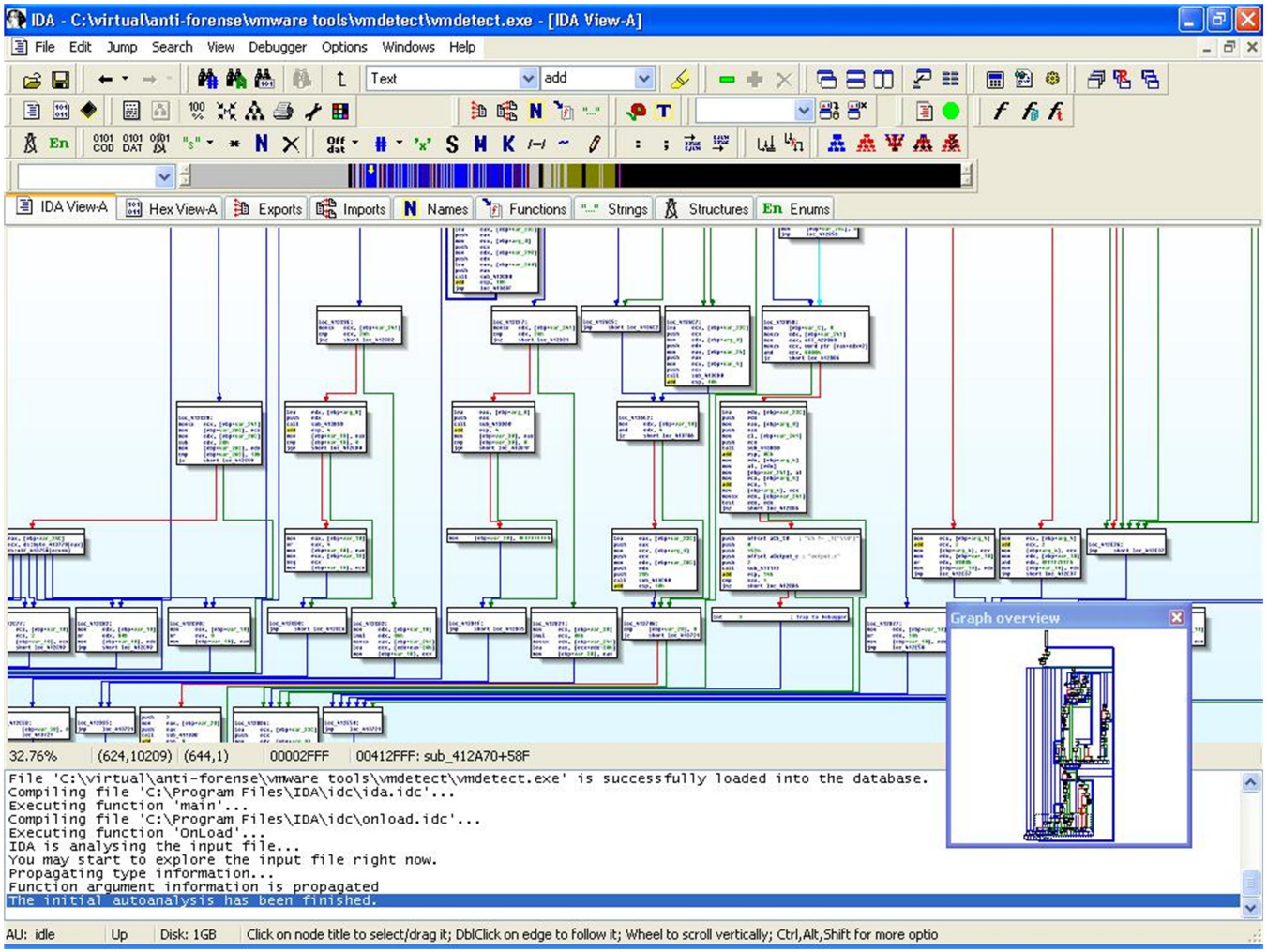
- Dificultar a compreensão do código assembly
- Diminuir o tamanho do artefato

Empacotamento do código binário

Exemplos de packers:

- UPX
- ASPack
- PECompact
- yoda's Crypter
- tELock
- Alguns compiladores

Empacotamento do código binário



Detecção do uso de depurador

Funções de um depurador:

- Execução passo a passo de um programa
- Valores de variáveis em um determinado instante da execução
- Laços de código que o programa executa e quantas vezes ele executa
- Resultados dos testes condicionais

Detecção do uso de depurador

Como a detecção é feita:

- Utilizando a função isDebuggerPresent()
- Utilizando um processo protetor

Detecção do uso de depurador

Programa que utiliza a função isDebuggerPresent():

```
#include ( windows.h )
int main ()
{
if (IsDebuggerPresent())
printf(”Está sendo executado em um depurador”);
else
printf(”Não está sendo executado em um depurador”);
return 0;
}
```

Detecção do uso de depurador

Solução:

- Editar o código assembly alterando a resposta do teste condicional

Detecção do uso de depurador

Programa que utiliza um processo protetor:

- Para depurar um programa é necessário utilizar uma porta específica
- Um programa em execução pode ser depurado por apenas um depurador

Detecção do uso de depurador

Programa que utiliza um processo protetor:

- Para depurar um programa é necessário utilizar uma porta específica
- Um programa em execução pode ser depurado por apenas um depurador

Detecção do uso de depurador

O que o artefato faz:

- Cria um processo para depurar ele mesmo
- Outro processo que tentar depurá-lo não irá conseguir

Detecção do uso de depurador

O que o artefato faz:

- Cria um processo para depurar ele mesmo
- Outro processo que tentar depurá-lo não irá conseguir

Detecção do uso de depurador

O que o analista faz:

- Altera o código assembly

Índice

Principais resultados.

- Coleta de mais de 3.300 artefatos
- Análise automatizada e geração de relatórios (uma análise a cada 7 minutos)
- Desenvolvimento de técnicas para analisar artefatos que utilizam novas tecnologias

Principais resultados.

- Coleta de mais de 3.300 artefatos
- Análise automatizada e geração de relatórios (uma análise a cada 7 minutos)
- Desenvolvimento de técnicas para analisar artefatos que utilizam novas tecnologias

Principais resultados.

- Coleta de mais de 3.300 artefatos
- Análise automatizada e geração de relatórios (uma análise a cada 7 minutos)
- Desenvolvimento de técnicas para analisar artefatos que utilizam novas tecnologias

Índice

Projetos em andamento

- Aperfeiçoamento dos scripts desenvolvidos e das ferramentas criadas
- Desenvolvimento de ambientes de análise para tipos de artefatos específicos
- Pesquisa por novas ferramentas, tecnologias e métodos de coleta

Apoio:

UNICAMP

Contato: angelocmcarvalho@gmail.com
Dario.Fernandes@cenpra.gov.br