Metodologia para Análise de Tráfego de Gerenciamento SNMP

Ewerton Monteiro Salvador

Grupo de Redes de Computadores
Instituto de Informática - UFRGS

26/06/2006

Agenda

- Introdução
- Objetivos
- Metodologia da análise
- Análise dos tráfegos SNMP
- Submissão de *traces* SNMP

Introdução

- *Simple Network Management Protocol* (SNMP) surgiu no final dos anos 80
- IETF (*Internet Engineering Task Force*)
  - Suporta leitura/escrita de informação de gerenciamento
- Na prática, SNMP utilizado como ferramenta de monitoração
  - Questões de segurança
- Atualmente se encontra na versão 3 (SNMPv3)

Introdução

- Apesar do SNMP ser amplamente conhecido, ainda não está claro:
  - Quais características são efetivamente utilizadas?
  - Como o SNMP se comporta em diferentes tipos de redes ou organizações?
  - Quais informações são mais freqüentemente solicitadas?
  - Quais são os padrões de interação típicos nas redes em produção do “mundo real”?

Introdução

- Proposta uma metodologia para coleta e análise de tráfego SNMP
  - "SNMP Traffic Measurements", *Internet Draft*
  - IRTF (*Internet Research Task Force*)
    - NMRG (*Network Management Research Group*)

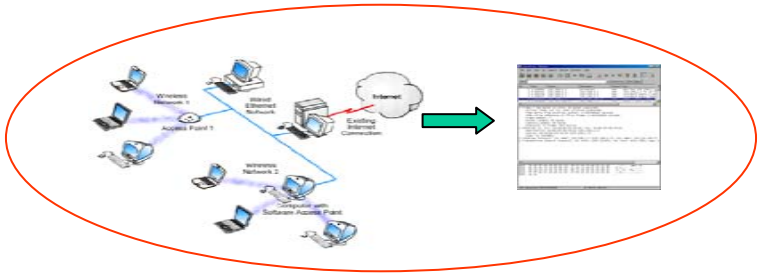
Objetivos

- Identificar padrões típicos de uso
- Entender o uso real do SNMP
- Demonstrar a simplicidade da metodologia proposta pelo *draft*
- Buscar novos parceiros para colaborarem com a pesquisa em andamento

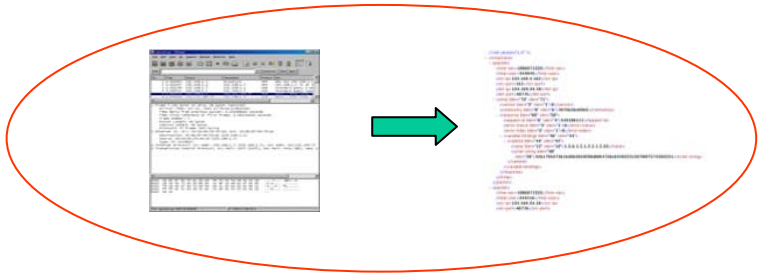
Metodologia da análise

- Composta de 5 etapas
- Auxílio de ferramentas desenvolvidas especialmente para esse estudo

Metodologia da análise



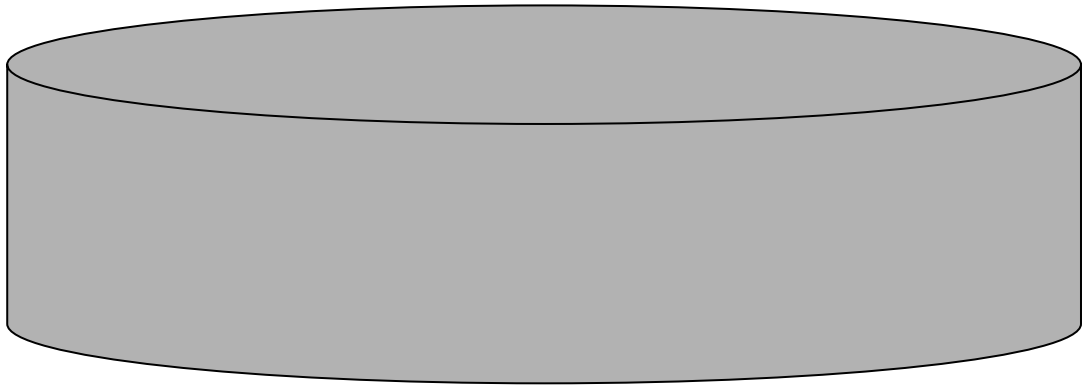
1. Capturar *traces* de tráfego SNMP



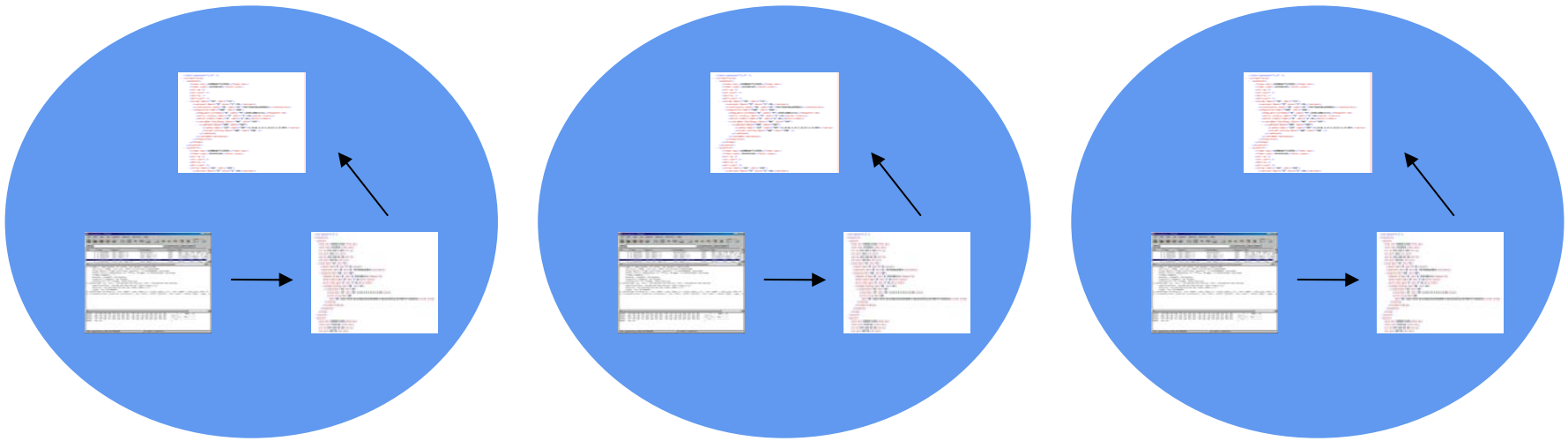
2. Converter traces em estruturas legíveis

3. Filtrar os dados convertidos

Metodologia da análise

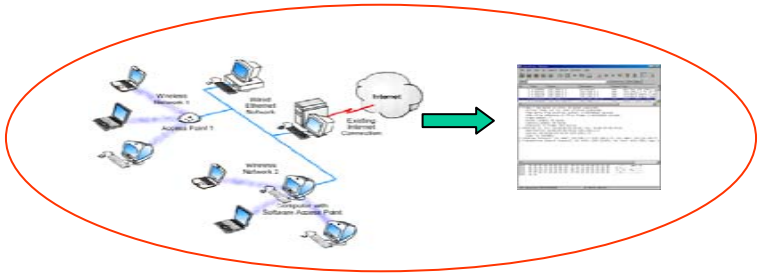


Repositório central

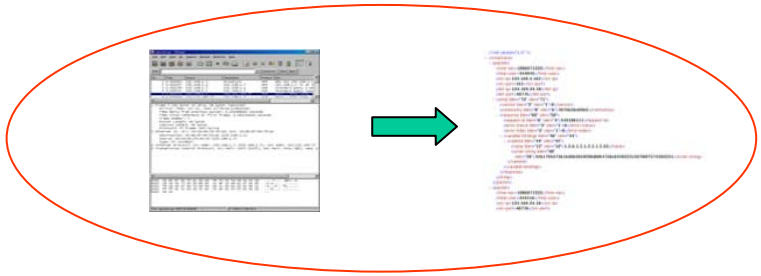


Domínios administrativos

Metodologia da análise

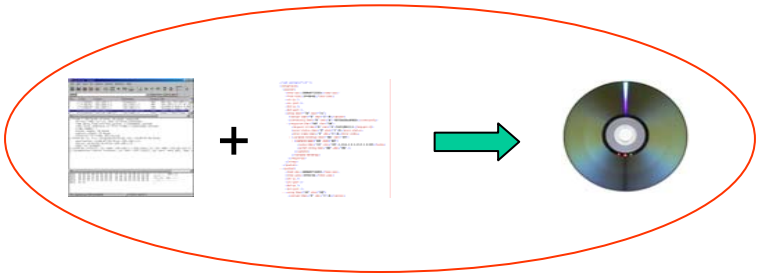


1. Capturar *traces* de tráfego SNMP

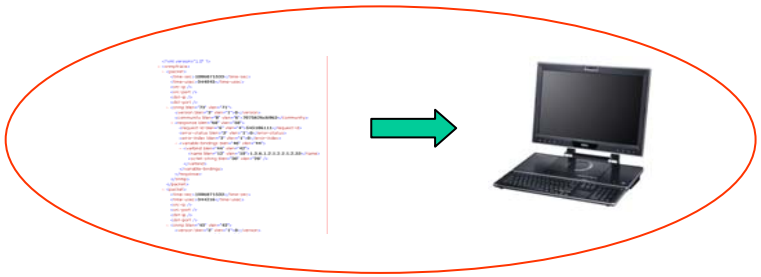


2. Converter traces em estruturas legíveis

3. Filtrar os dados convertidos



4. Armazenar os traces em um repositório estável



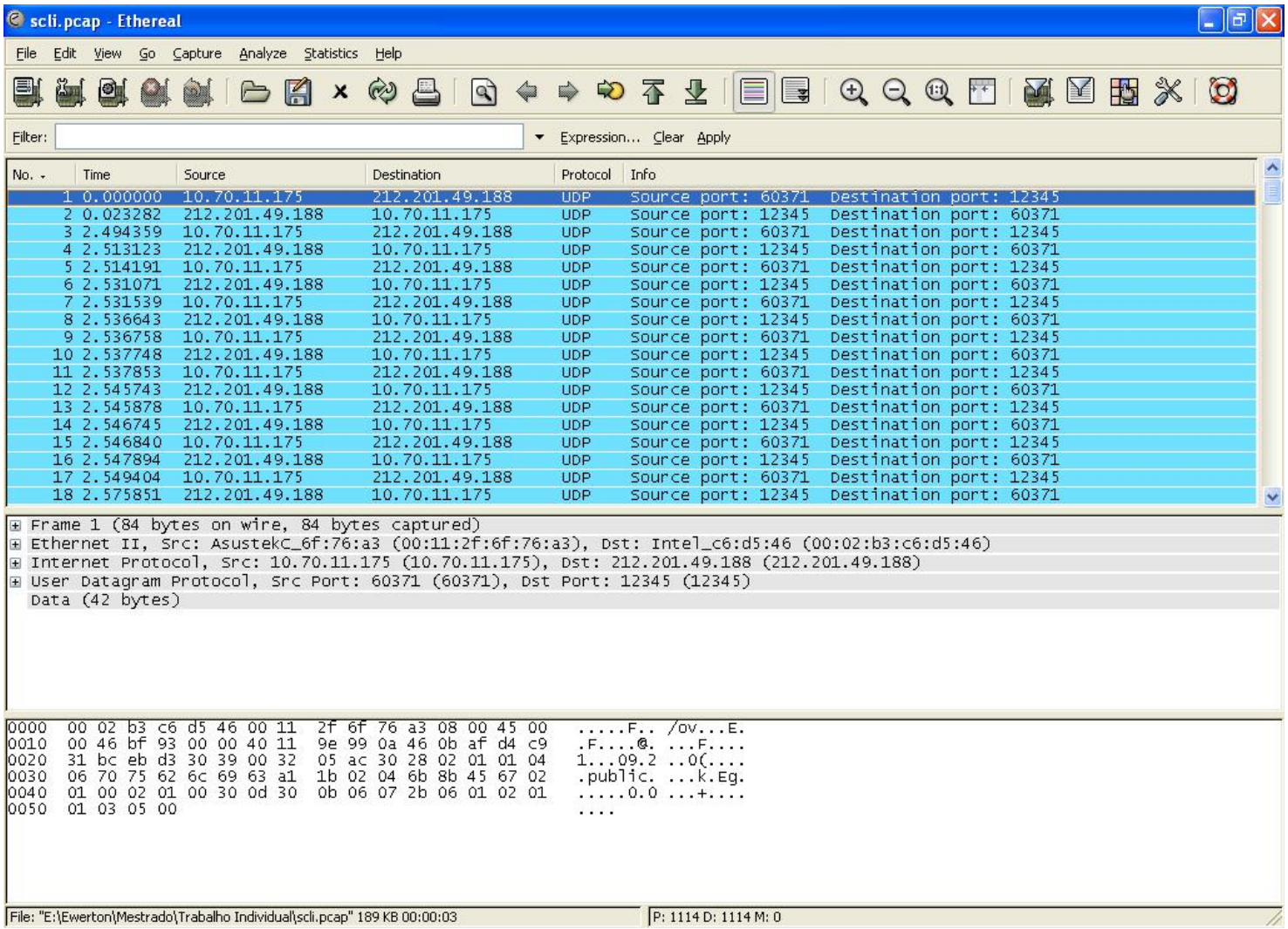
5. Analisar os dados convertidos

Metodologia da análise

1. Capturando *traces* do tráfego SNMP

- *Packet Sniffers* (TCPDUMP, etc.)
- Duração: pelo menos uma semana
- Escolha do ponto de coleta do tráfego SNMP (local estratégico)
- Metadados relacionados para cada *trace*

Metodologia da análise



Arquivo pcap contendo tráfego SNMP monitorado

Metodologia da análise

2. Conversão dos *traces*

- XML (*eXtended Markup Language*) - facilidade de leitura tanto para seres humanos quanto para máquinas
- CSV (*Comma Separated Values*) - alternativa "enxuta" à explosão da representação XML
- SNMPDUMP - ferramenta que trabalha tanto com XML quanto com CSV

Metodologia da análise

```
<?xml version="1.0" ?>
- <snmptrace>
  - <packet>
      <time-sec>1147212206</time-sec>
      <time-usec>739609</time-usec>
      <src-ip>10.70.11.175</src-ip>
      <src-port>60371</src-port>
      <dst-ip>212.201.49.188</dst-ip>
      <dst-port>12345</dst-port>
    - <snmp blen="42" vlen="40">
        <version blen="3" vlen="1">1</version>
        <community blen="8" vlen="6">7075626c6963</community>
      - <get-next-request blen="29" vlen="27">
          <request-id blen="6" vlen="4">1804289383</request-id>
          <error-status blen="3" vlen="1">0</error-status>
          <error-index blen="3" vlen="1">0</error-index>
        - <variable-bindings blen="15" vlen="13">
          - <varbind blen="13" vlen="11">
              <name blen="9" vlen="7">1.3.6.1.2.1.1.3</name>
              <null blen="2" vlen="0" />
            </varbind>
          </variable-bindings>
        </get-next-request>
      </snmp>
    </packet>
  - <packet>
      <time-sec>1147212206</time-sec>
      <time-usec>762891</time-usec>
      <src-ip>212.201.49.188</src-ip>
      <src-port>12345</src-port>
      <dst-ip>10.70.11.175</dst-ip>
      <dst-port>60371</dst-port>
    - <snmp blen="47" vlen="45">
```

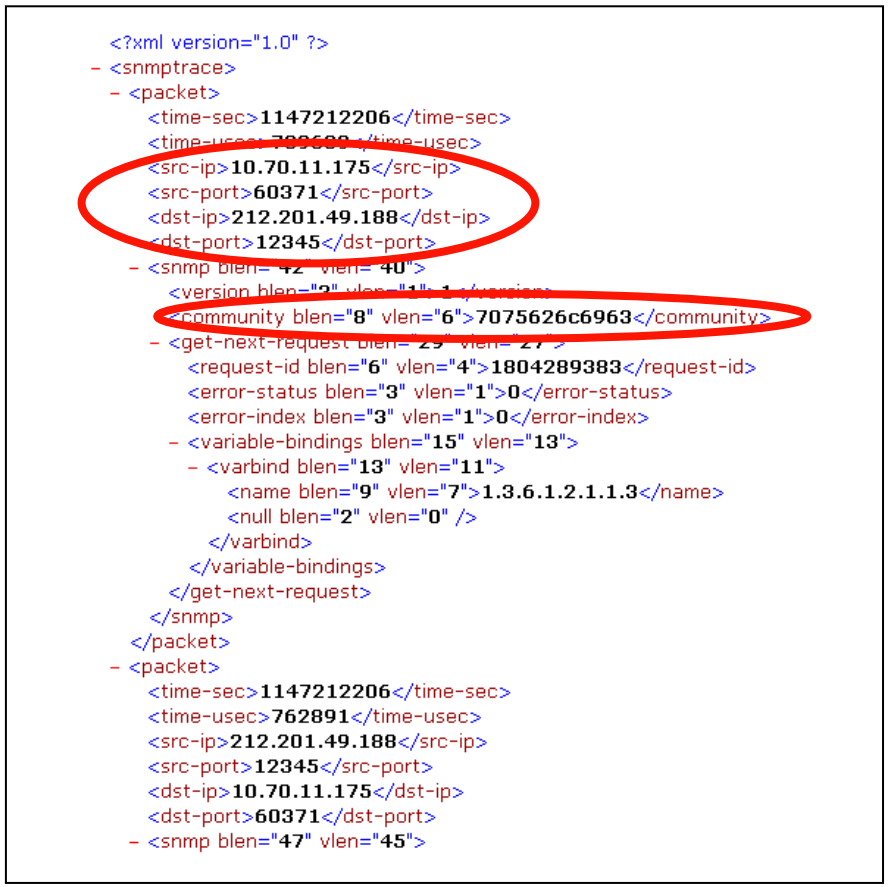
***Trace* convertido para o formato XML**

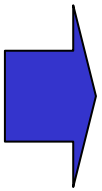
Metodologia da análise

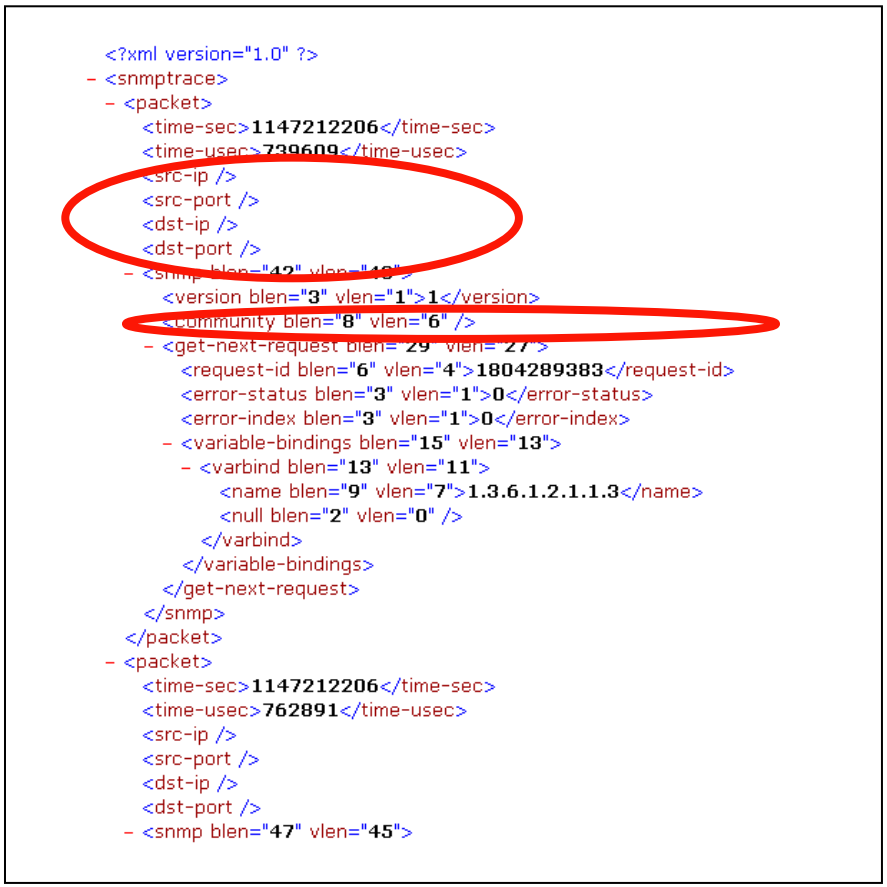
3. Filtrando os *traces*

- Anomimização (remoção dos dados considerados sensíveis)
  - IPs origem e destino
  - Portas origem e destino
  - String de comunidade
  - Valores dos objetos das MIBs
- Filtragem realizada através da manipulação da representação XML do tráfego
- SNMPDUMP – também faz anonimização

Metodologia da análise







Representação XML normal e anonimizada

Metodologia da análise

4. Armazenando os traces

- Necessidade de armazenamento do arquivo PCAP e da sua representação XML/CSV
- Necessário para eventuais futuras verificações/correções

Metodologia da análise

5. Processando os traces

- Processamento da representação XML/CSV realizado através de scripts de análise
- Preferencialmente será utilizada a linguagem Perl (pacote XML::LibXML)

Análise dos tráfegos SNMP

- Várias questões relacionadas ao protocolo SNMP poderão ser respondidas
- Muitas dessas questões já foram propostas pelo *draft*
- Outras ainda poderão ser adicionadas ao estudo

Análise dos tráfegos SNMP

- **Questões propostas**
  - Estatísticas básicas
  - Tráfego periódico vs. aperiódico
  - Tamanho da mensagem e distribuição da latência
  - Níveis de concorrência
  - Abordagens para leitura de tabelas

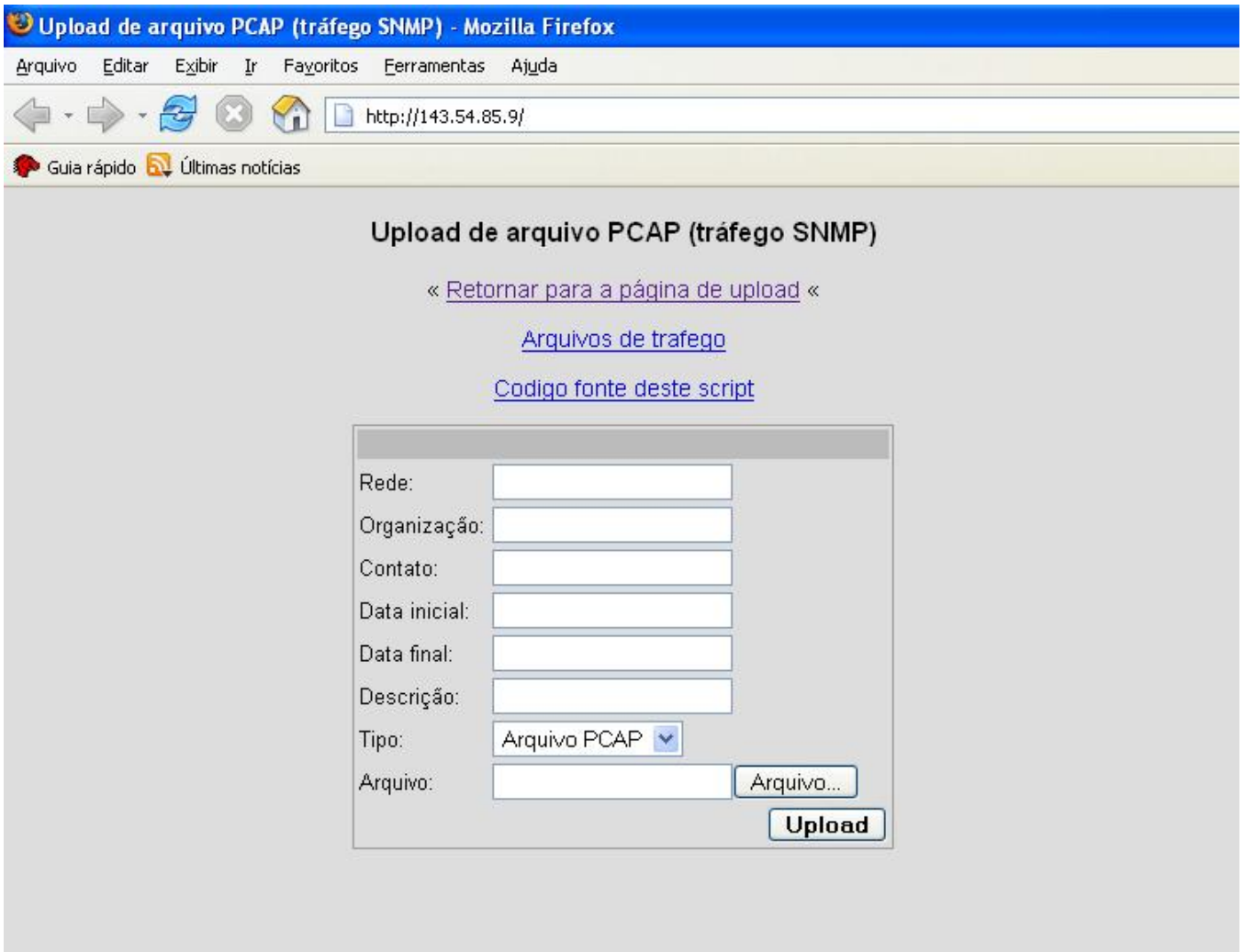
Análise dos tráfegos SNMP

- **Questões propostas**
  - *Pollings* baseadas em *traps*
  - MIBs populares
  - Uso de objetos obsoletos
  - Distribuição do tamanho da codificação

Submissão de *traces* SNMP

- Administradores são fortemente incentivados a contribuírem com amostras de tráfego SNMP
- Processo de submissão dos pcaps e geração do arquivo XML facilitado através de uma página Web
- Opção de instalação do ambiente de anonimização em sua própria rede
  - Total controle sobre o tratamento dos *traces*
- Suporte é oferecido pelo Grupo de Redes de Computadores da UFRGS

Submissão de *traces* SNMP



Site para upload, conversão em XML e anonimização dos arquivos *pcaps*

Contato

Ewerton Monteiro Salvador

E-mail: emsalvador@inf.ufrgs.br

Sala 210 – Instituto de Informática - UFRGS