# ESTUDO COMPARATIVO DE FERRAMENTAS ANALISADORAS DE PACOTES EM REDE TPC/IP

Felipe Santos Couto, Alex Ferreira dos Santos e Agnaldo Volpe Lovato
Universidade Estadual do Sudoeste da Bahia (UESB)
felipe_couto@yahoo.com.br, afsantos@uesb.edu.br, agnaldovl@yahoo.com.br

**Resumo**

A segurança com as informações trafegadas em redes de computadores tem se tornado um fator de considerável preocupação, pois, com o aumento do uso de computadores e da Internet, houve um crescimento do número de incidentes ocorridos nesses ambientes informatizados. Muitos desses incidentes podem causar a lentidão da rede ou até ao acesso a informações confidenciais. Para ter uma visão do que está acontecendo em uma rede, faz-se uso de softwares analisadores de pacotes. Os analisadores de pacotes capturam e apresentam todo o fluxo de dados trafegados, decodificando e exibindo o conteúdo dos pacotes para uma análise detalhada. Existem diversas ferramentas analisadoras de pacotes, tanto ferramentas livres quanto ferramentas proprietárias. O presente trabalho apresenta um estudo comparativo envolvendo duas ferramentas analisadoras de pacotes proprietárias e duas livres, com o objetivo de apresentar suas funcionalidades, assim como, suas vantagens e desvantagens.

**Palavras-chave:** Incidentes de segurança. Segurança da Informação. Pacotes de rede. Analisador de pacotes.

**Abstract**

The security of information traffic over networks of computers has become a factor of considerable concern, because with the increasing use of computers and the Internet, there was a growing number of incidents in these computing environments. Many of these incidents can cause delays of the network or even provide access to confidential information. To get an overview of what is happening on a network makes use of software packet analyzers. The packet analyzers capture and present all the data traffics flow decoding and displaying the contents of the package for detailed analysis. There are several tools packet analyzer, both free tools and proprietary tools. This paper presents a comparative study involving two proprietary tools packet analyzer and two free, in order to present the features and their advantages and disadvantages.

**Keywords:** Security Incidents. Information Security. Network Packets. Packet Analyzer.

## 1. Introdução

O desenvolvimento de aplicações que utilizam redes de computadores juntamente com o crescente número de usuários, contribuiu e ainda contribui para o crescimento da Internet. Com toda a facilidade de comunicação oferecida pela Internet, as organizações passaram, cada vez mais, a utilizar os serviços oferecidos por ela. Visto que, informações confidenciais estavam sendo trafegadas pela rede, a preocupação com a segurança dessas informações foi despertada, pois estas poderiam estar expostas a usuários mal-intencionados. Além do acesso improvável e indesejável de usuários mal-intencionados, a entrada de pacotes de dados maliciosos em uma rede também é de grande preocupação quanto à segurança da mesma (CORRÊA, 2011), (SILVA, 2009), (BANERJEE, 2010).

A análise de pacotes poderá auxiliar no entendimento das características de rede,

saber quem tem acesso, determinar quem ou o que está utilizando largura de banda disponível, identificar horários de mais utilização da rede, identificar possíveis ataques ou atividades maliciosas, dentre outras coisas. Assim, faz-se indispensável um monitoramento sobre os eventos anormais ocorridos nas redes de computadores. Este monitoramento é feito através de ferramentas analisadoras de pacotes (SANDERS, 2007).

Neste trabalho será apresento um estudo comparativo envolvendo duas ferramentas analisadoras de pacotes proprietárias e duas livres, com o objetivo de apresentar suas funcionalidades, assim como, suas vantagens e desvantagens.

As próximas seções deste artigo estarão organizadas da seguinte maneira: Na seção 2 será abordado aspectos da segurança da informação. A seção 3descreve os analisadoras de pacotes. Na seção 4 apresentamos as ferramentas utilizadas. Na seção 5 será apresentado o cenário utilizado. A seção 6 conterá o estudo comparativo e na seção 7 a análise comparativa dos resultados. Por fim, na seção 8 estarão as considerações finais.

## 2. Segurança da Informação

Um dos acontecimentos mais importantes da década de 1990 foi o surgimento da *World Wide Web* (WWW), tornando possível o acesso a Internet aos diversos tipos de usuários espalhados pelo mundo. Além disso, a Web serviu também como meio para habilitar e disponibilizar diversas novas aplicações, incluindo serviços bancários on-line, serviços multimídia em tempo real e serviços de recuperação de informações (KUROSE; ROSS, 2006).

No Brasil, o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) é o órgão responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira. Além do processo de tratamento aos incidentes, o CERT.br também atua conscientizando os usuários da Internet sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet no Brasil. O objetivo estratégico dessas atividades é possibilitar o aumento dos níveis de segurança e da capacidade de tratamento de incidentes das redes no país (CERT.br, 2011).

A informação se tornou um bem essencial tanto para uma organização quanto para as pessoas. Por este motivo, se faz necessário a utilização de algum tipo de proteção. Com a Internet os computadores estão cada vez mais interconectados. Diante desse exponencial crescimento, a informação se torna vulnerável, diante de uma grande variedade de ameaças (NBR ISO/IEC 27002, 2005).

Nakamura e Geus (2007), afirmam que a necessidade de segurança é um fato que vem transcendendo o limite da produtividade e da funcionalidade. Enquanto a velocidade e a eficiência em todos os processos de negócios significam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em grandes prejuízos e falta de novas oportunidades de negócios.

A Segurança da Informação se dá através da implementação de um conjunto de controles adequados, que inclui políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos (NBR ISO/IEC 27002, 2005).

Segundo Comer (2007), aspectos de segurança devem ser levados em consideração, como por exemplo:

- Confidencialidade: Consiste na proteção da informação contra o acesso não autorizado;
- Integridade: Consiste na proteção da informação contra qualquer modificação da mesma por alguém não autorizado;

- Disponibilidade: Consiste em garantir que a informação esteja sempre disponível para os usuários autorizados.

Logo, qualquer ambiente que possua conexão com a Internet esta sujeito a riscos. Assim, percebemos o quanto é importante a utilização da segurança das informações, e mais especificamente, a importância do uso de ferramentas que auxiliam na detecção de violações de segurança.

## 3. Analisadores de Pacotes

Os analisadores de pacotes capturam e apresentam todo o fluxo de dados trafegado decodificando e exibindo o conteúdo dos pacotes para uma análise detalhada (COMER, 2007). Existem diversos tipos de ferramentas que capturam e analisam os pacotes de dados trafegados na rede, incluindo tanto as livres e as proprietárias.

A segurança de uma rede implica na segurança dos pacotes de dados, que é o bloco mais básico de comunicação, a fim de transmitir informações de um dispositivo para outro. Um pacote de dados está contido no segmento de dados que contém diversas informações, como o protocolo a ser utilizado, o endereço de hardware de destino, entre outras (BANERJEE, 2010).

A identidade de um pacote pode ser detectada através do estudo do seu conteúdo. Este estudo de detectar e visualizar o conteúdo de um segmento de dados e seu pacote é denominado como *packet sniffing*(BANERJEE, 2010).

A análise de pacotes apresenta o processo de captura e interpretação de dados que flui através de uma rede, a fim de entender melhor o que está acontecendo nela. Essa análise de pacotes é normalmente realizada por uma ferramenta analisadora de pacotes (SANDERS, 2004).

Um analisador de pacotes é um software ou hardware que cuja funcionalidade é monitorar, interceptar e capturar o fluxo de tráfego de uma rede. Geralmente, uma placa de rede aceita apenas os pacotes de entrada que são destinados especificamente para ela. Porém quando a placa de rede é colocada em modo promíscuo, ela aceitará todos os pacotes de entrada, independentemente de seus destinos pretendidos. É possível, também, determinar quais pacotes capturar, através do uso de filtros (MARCELLA, 2008).

A maioria dos analisadores de pacotes também são analisadores de protocolos, ou seja, podem montar fluxos de pacotes individuais e decodificar as comunicações que utilizam de diferentes protocolos. Além de analisar o tráfego atual da rede, os arquivos de pacotes que foram gravados na captura anterior também poderão ser analisados de maneira compreensível (MARCELLA, 2008).

## 4. Ferramentas utilizadas

Para a escolha das ferramentas proprietárias foi observado relevância (verificação das ferramentas mais utilizadas no mercado) e disponibilidade para download dessas ferramentas. As ferramentas livres escolhidas são as ferramentas mais utilizadas.

Dentre as ferramentas listadas, foram escolhidas quatro para a realização do estudo: *TCPdump* e *Wireshark* (software livre),*Capsa Network Analyzer* e *CommView* (software proprietário).

### *A. Capsa Network Analyzer*

*Capsa Network Analyzer* (Figura 1) é um analisador de pacotes, fornecido pela Colasoft, que auxilia os administradores de rede a detectar e solucionar problemas ocorridos na rede, melhorar o seu desempenho e aumentar a sua segurança. De acordo com o seu manual, disponível no site da Colasoft (www.colasoft.com), o *Capsa Network Analyzer* possui habilidades de captura em tempo real de pacotes, decodificação e análise dos pacotes capturados, geração de diagnósticos automáticos de eventos na rede. Com um poderoso filtro e exibição informações estatísticas, Capsa permite que o usuário encontre, de forma rápida e eficiente, o que deseja em sua rede.

Para esse estudo foi utilizado o *Capsa Network Analyzer Enterprise* (versão Demo).

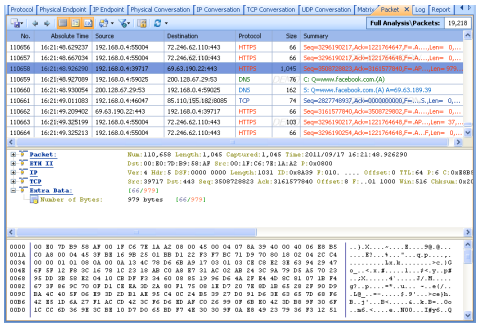

**Figura 1. Tela do Capsa Network Analyzer**

*B. CommView*

De acordo com o site da TamoSoft (www.tamos.com), o *CommView* (Figura 2) é um poderoso monitor e analisador de redes, destinados a administradores de redes, profissionais de segurança, até mesmo um simples usuário da Internet que queira uma imagem completa do tráfego de sua rede. Com uma interface amigável, *CommView* combina performance e flexibilidade, com a facilidade de uso.

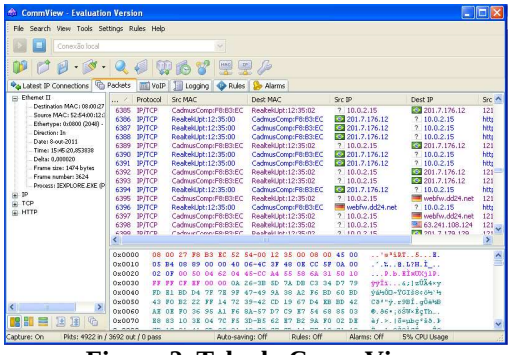

**Figura 2. Tela do CommView**

Além de funções como examinar, armazenar, filtrar, importar e exportar pacotes capturados, ver protocolos decodificados, o *CommView* inclui um analisador de VoIP para uma análise aprofundada deste tipo de serviço. Os pacotes capturados podem ser salvos em arquivos de *logs* para análise futura. Com o sistema de filtragem de pacotes, torna-se possível descartar os pacotes que o usuário não utiliza, ou até mesmo capturar somente aqueles desejados. Alarmes configuráveis notificam sobre acontecimentos importantes, tais como: pacotes suspeitos, utilização de largura de banda alta, ou endereços desconhecidos.

Para esse estudo foi utilizado o *CommView* 6.1 (versão para avaliação).

*C. Tcpdump*

O*Tcpdump* (Figura 3) é uma ferramenta cujo principal objetivo é analisar o tráfego que flui através da rede. Baseia-se na biblioteca de captura pcap e funciona através de linha de comando. Por ser flexível às necessidades do administrador, o *Tcpdump* permite que a interface de rede desejada para a execução do monitoramento seja especificada, assim como as de portas de origem ou destino e os protocolos que serão monitorados. O *Tcpdump* é capaz de trabalhar com arquivos, tornando possível a analise dos pacotes capturados utilizando filtros após o monitoramento do tráfego da rede. Todas as informações e downloads do *Tcpdump*pode ser encontrado em (www.tcpdump.org)


**Figura 3. Tela do Tcpdump**

*D. Wireshark*

*Wireshark* (Figura 4) é um dos mais populares analisadores de pacotes de rede. Possui conjunto de poderosos recursos e funciona na maioria das plataformas de computação, incluindo Windows, OS X, Linux e UNIX. Está disponível gratuitamente como *open source* em (www.wireshark.org), e é distribuído sob a versão GNU General Public License 2 (BANERJEE, 2010).

É capaz de capturar, visualizar e analisar os pacotes de dados, além de fornecer suporte *wireless* que auxilia aos administradores a solucionar problemas de redes sem fio. Dessa forma, o *Wireshark* é capaz decodificar os pacotes em um formato que ajuda os administradores a rastrear problemas que estão causando o mau desempenho na rede, a conectividade

intermitente, e outros problemas comuns (SANDERS, 2007).

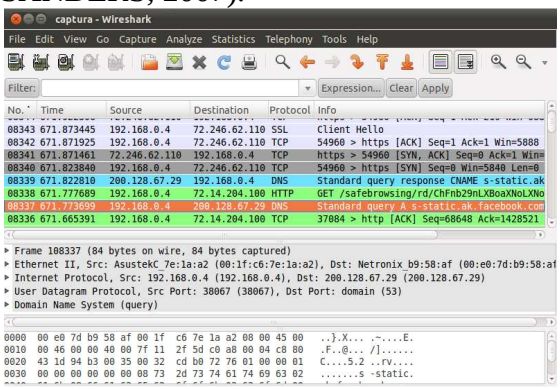


**Figura 4. Tela do Wireshark**

## 5. Cenário

As ferramentas escolhidas foram submetidas ao monitoramento da rede, no qual, três computadores estarão conectados em um servidor de compartilhamento de Internet. As ferramentas foram instaladas no próprio servidor a fim de capturar os pacotes das três máquinas clientes (Figura 5).

Pretende-se acessar sites e aplicações diversas para alimentar as ferramentas com dados. Todas as ferramentas foram configuradas para não utilizar filtros de pacotes durante a captura.

No servidor de compartilhamento de Internet está instalado o Ubuntu 10.10. Para a execução das ferramentas que trabalham em ambiente Windows, foi feito a virtualização do Windows XPSP3 utilizando a ferramenta VirtualBox.

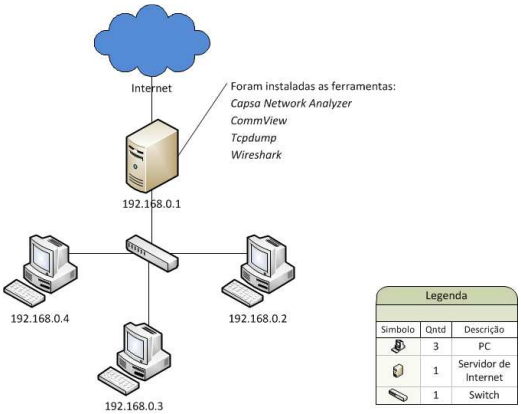


**Figura 5. Topologia da rede do cenário**

## 6. Estudo comparativo

Nesta seção serão descritas as funcionalidades das ferramentas analisadoras de pacotes escolhidas, observando duas características principais: a utilização de filtros e geração de estatísticas.

### ✓ *Filtragem de pacotes*

Os filtros permitem mostrar apenas os pacotes particulares em uma captura de dados. Pode-se criar e usar uma expressão para encontrar exatamente o que se deseja em uma captura. Para facilitar o uso de filtro é imprescindível o conhecimento da sintaxe.

#### *A. Capsa Network Analyzer*

A caixa de diálogo *Filter* (Figura 6) é dividida em três partes:

- *Filterlist*: lista todos os filtros disponíveis, incluindo os que foram criados pelo usuário.
- *FilterFlow-chart*: Mostra o fluxograma dos filtros. É atualizado a cada modificação no *Filterlist.*
- *Buttons*: Apresenta botões com a finalidade de adicionar, modificar, deletar, importar e exportar filtros. Além do botão para redefinir a lista de filtros.

É possível criar filtros simples baseados em endereços, portas ou protocolos em um único filtro.

Os filtros avançados possuem mais condições do que os filtros simples permitindo definir parâmetros precisos como valores, tamanhos e padrões dos pacotes que serão capturados.

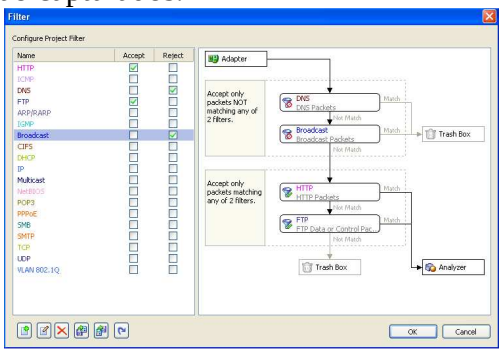


**Figura 6. Tela da janela Filter do Capsa Network Analyzer**

#### *B. CommView*

As opções de filtragem no *CommView* se localizam na aba *Rules*, que permite que você defina regras para a captura. Os pacotes serão filtrados com base nas regras definidas.

Há oito tipos de regras que são exibidos e descritos na Tabela 1.

| Regras | Descrição |
|---|---|
| *Protocols&Direction* | Permite capturar ou ignorar pacotes baseados nos protocolos e na sua direção. |
| *MAC Addresses* | Permite capturar ou ignorar pacotes baseados nos endereços MAC |
| *IP Addresses* | Permite capturar ou ignorar pacotes baseados nos endereços Ips |
| *Ports* | Permite capturar ou ignorar pacotes baseados nas portas |
| *TCP Flags* | Permite capturar pacotes baseados nas flags TCP |
| *Text* | Permite capturar pacotes que contêm determinado texto |
| *Process* | Permite capturar pacotes baseados no nome do processo |
| *Advanced* | Permite criar filtros complexos utilizando lógica boolena |

**Tabela 1. Tipos de regras de filtragem do Commview**

As Tabelas 2, 3 e 4 mostram, respectivamente, os operadores de comparação, lógico e exemplos de expressões que são utilizados no *CommView*:

| Operadores | Descrição |
|---|---|
| = | Igual a |
| != e <> | Diferente de |
| > | Maior que |
| < | Menor que |
| >= | Maior ou igual a |
| <= | Menor ou igual a |

**Tabela 2: Operadores de comparação do Commview.**

| Operadores | Descrição |
|---|---|
| and | Ambas as condições devem ser verdadeiras |
| or | Qualquer uma das condições deve ser verdadeira |
| not | Nenhuma codição é verdadeira |

**Tabela 3: Operadores lógicos do Commview.**

| Expressão | Descrição |
|---|---|
| dir!=in | Mostra todo o tráfego de chegada |
| not (ipproto=dns) | Mostra tudo exceto o tráfego DNS |
| size in 200..600 | Mostra todos os pacotes com tamanhos entre 200 e 600 bytes |
| dip=192.168.0.1 | Mostra todo o tráfego destinado para 192.168.0.1 |

**Tabela 4: Exemplo de expressões de filtro do Commview.**

### *C. Tcpdump*

Uma das principais funcionalidades do *Tcpdump* é o uso de filtros. É possível criar diversos tipos de filtros utilizando parâmetros, como por exemplo, porta de destino e origem, protocolos, endereços IP e MAC. Além disso, o *Tcpdump* possibilita a combinação dos filtros.

A Tabela 5apresenta os operadores lógicos. A Tabela 6exemplifica algumas expressões de filtragens que podem ser utilizadas no *Tcpdump*.

| Operadores | Descrição |
|---|---|
| ! ounot | Negação |
| && ou and | Concatenação |
| \|\| ou or | Alternação |

**Tabela 5: Operadores lógicos do Tcpdump.**

| Expressões | Descrição |
|---|---|
| tcpdump -i eth0 -p net 192.168 | Mostra somente o tráfego da rede 192.168 que estiver passando na interface eth0. |
| tcpdump -i eth0 -p net 192.168 and dst port 80 | Mostra todo o tráfego da rede 192.168 com destino a porta 80 |
| tcpdump -i eth0 -p icmp | Mostra somente os pacotes icmp na rede |
| tcpdump -i eth0 -p net 192.168 and not port 80 | Mostra o tráfego na rede 192.168 com exceção da porta 80 |

**Tabela 6: Exemplos de expressões de filtros do Tcpdump**

### *D. Wireshark*

O *Wireshark* oferece dois tipos de filtros: os filtros de captura e os filtros de exibição. Os filtros de captura são aqueles que são configurados antes de iniciar o processo de captura de pacotes. Ao invés de capturar todo o tráfego da rede, somente serão capturados os pacotes relacionados ao filtro, os demais serão descartados. Os filtros de exibição são aqueles que são aplicados a um arquivo de captura, uma vez que o arquivo foi criado, com a finalidade de exibir apenas os pacotes que correspondem a esse filtro.

Filtros de exibição são mais comumente usados do que os filtros de captura, pois eles permitem a filtragem de pacote sem descartar o restante dos dados no arquivo de captura. Assim, caso necessite voltar à

captura original, basta apagar a expressão de filtro.

A caixa de diálogo *Capture Filter* (Figura 7), apresenta uma lista de todos os campos possíveis de protocolo no lado esquerdo da janela. Estes campos especificam todos os possíveis critérios de filtro. Para usuários mais experientes, poderá ser criado um filtro personalizado, seguindo a regra da sintaxe do programa.

As Tabelas 7, 8 e 9 mostram os operadores de comparação, lógico e exemplos de expressões que são utilizados no *Wireshark.*

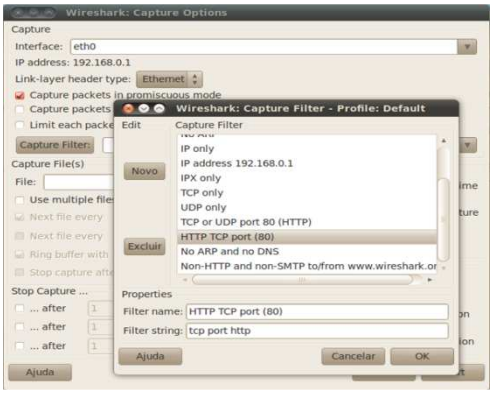


**Figura 7: Tela de configuração de filtros do Wireshark.**

| Operadores | Descrição |
|---|---|
| == | Igual a |
| \|= | Diferente de |
| > | Maior que |
| < | Menor que |
| >= | Maior ou igual a |
| <= | Menor ou igual a |

**Tabela 7: Operadores de comparação do Wireshark.**

| Operadores | Descrição |
|---|---|
| and | Ambas as condições devem ser verdadeiras |
| or | Qualquer uma das condições deve ser verdadeira |
| xor | Apenas uma condição deve ser verdadeira |
| not | Nenhuma codição é verdadeira |

**Tabela 8: Operadores lógicos do Wireshark.**

| Expressão | Descrição |
|---|---|
| host www.exemplo.com | Mostra todo o tráfego do host www.exemplo.com |
| !dns | Mostra tudo exceto o tráfego DNS |
| not broadcast and not multicast | Apenas mostra o tráfego unicast |
| ip.dst==192.168.0.1 | Mostra todo o tráfego destinado para 192.168.0.1 |

**Tabela 9: Exemplo de expressões de filtro do Wireshark.**

## ✓ *Geração de Estatísticas*

As estatísticas podem determinar qual o tamanho dos pacotes sendo transmitidos, detalhes das conversas realizadas entre os *hosts*, a largura de banda utilizada, assim, como o tempo de resposta das solicitações e gráficos do fluxo de pacotes trafegados.

### *A. Capsa Network Analyzer*

O *Capsa Network* apresenta diversos relatórios de estatísticas. Cada aba do programa apresenta informação sobre a rede. A seguir será apresentado alguns relatórios de estatísticas importantes.

A aba *Dashboard* (Figura 8) exibe gráficos e estatísticas que possibilitam uma visão geral do fluxo de dados que trafega pela rede.

A aba *Summary* (Figura 9) fornece estatísticas gerais sobre a rede. Ao selecionar o nó raiz será possível obter as estatísticas globais da rede. Ao selecionar apenas um nó específico, serão apresentadas informações específicas daquele nó, como por exemplo, número de pacotes trafegados e seus respectivos tamanhos em bytes, e quantidade bytes e pacotes por segundo.

Na aba Protocol é exibido uma estrutura hierárquica dos protocolos. Cada protocolo tem sua própria cor facilitando a sua identificação. Informações como total de bytes e quantidade de pacotes de cada protocolo são exibidas de acordo com a Figura 10.

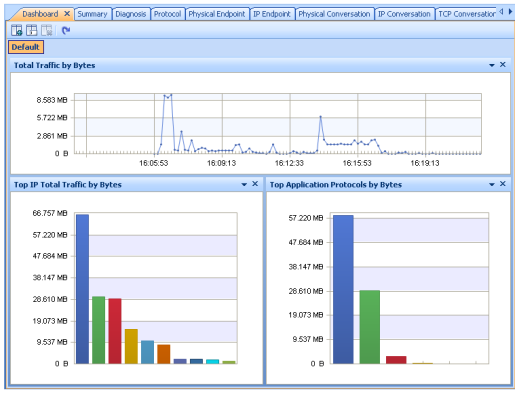


**Figura 8: Aba Dashboard do Capsa Network Analyzer.**

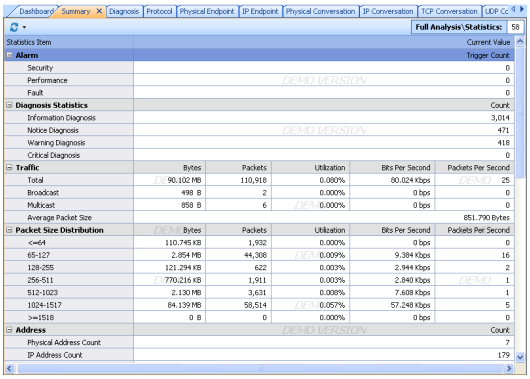

**Figura 9: Aba Summary do Capsa Network Analyzer.**

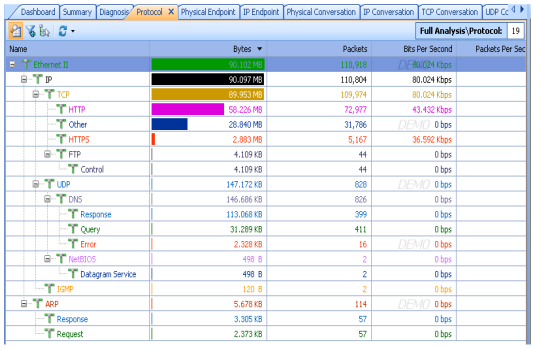

**Figura 10: Aba Protocol do Capsa Network Analyzer**

A aba *Matrix* (Figura 11) apresenta a visualização da análise das estatísticas de tráfego de rede em tempo real. Os nós são dispostos em uma elipse alongada e a espessura da linha indicar o volume de tráfego entre os nós. Além de possibilitar a visualização para uma rede global, é possível visualizar os nós de rede específica.

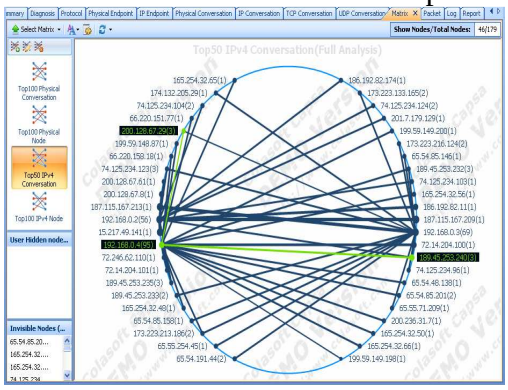

**Figura 11: Aba Matrix do Capsa Network Analyzer.**

As abas *Physical Endpoints* e IP Endpoints apresentam todos os hosts na rede. Todos os nós são divididos pelo endereço físico e o endereço IP.

Na aba *Pshysical Endpoints* é fornecido um grande número de estatísticas que auxilia a encontrar informações úteis sobre os endereços MAC. Na aba IP Edpoints é fornecido um grande número de estatísticas sobre os terminais IP auxiliando a encontrar informações úteis sobre os endereços IP.

A aba *Physical Conversation* e a aba IP Conversation fornecem estatísticas das conversas entre endereços MAC e IP, respectivamente. Cada conversa apresenta o respectivo endereço de origem e destino, os pacotes enviados e recebidos, tamanhos dos pacotes e a duração de comunicação.

A aba *TCP Conversation* e a aba *UDP Conversation* fornecem estatísticas das conversas TCP e UDP respectivamente. Cada conversa apresenta o endereço IP de origem e destino, a porta de origem e destino, os pacotes enviados e recebidos, tamanhos de pacotes e a duração de comunicação.

*B. CommView*

O ítem General (Figura 12) exibe os pacotes por segundo, um medidor da utilização de banda da rede, bem como a contagem de pacotes e bytes geral da captura.

A opção *Protocol* apresenta a distribuição dos protocolos Ethernet, tais como ARP, IP, entre outros. A opção IP Protocol (Figura 13) apresenta a distribuição dos protocolos IP. Já a opção IP Sub-protocol (Figura 14) apresenta a distribuição das principais sub-protoolos da camada de aplicação: HTTP, FTP, POP3, SMTP, NetBIOS, HTTPS e DNS.

A opção By MAC do ítem *Hosts* listas todos os hosts ativos na rede pelo seu endereço MAC e exibe as estatísticas de transferência de dados, como apresenta a Figura 15.

A opção My IP do ítem Matrix apresenta a matriz gráfica das conversas entre os *hosts* com base em seus endereços IP. Os *hosts* são colocados em círculo, e as sessões entre eles são mostradas como linhas que ligam os *hosts*, como é apresentado na Figura 16.

O item Errors (Figura 17) exibe as informações sobre os erros ocorridos na rede.

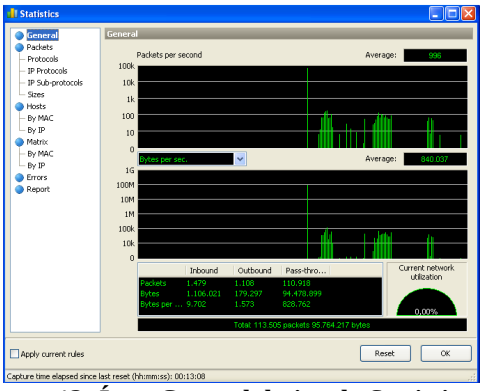


**Figura 12: Ítem General da janela Statistics do CommView.**

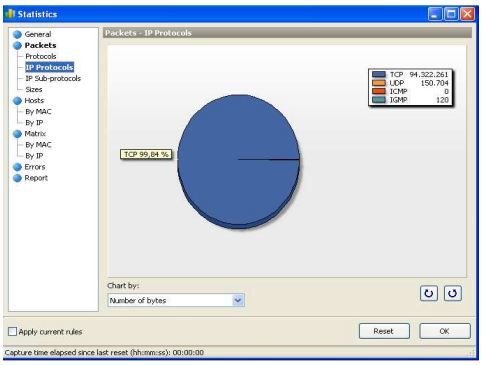


**Figura 13: Opção IP Protocol da janela Statistics do CommView.**

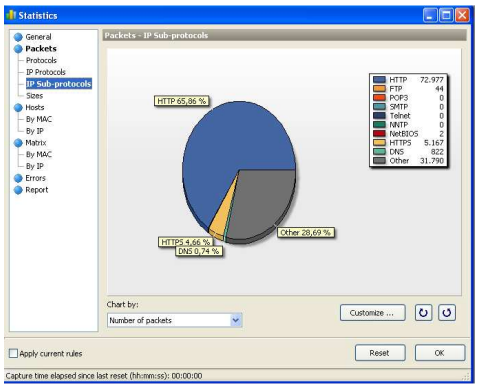


**Figura 14: Opção IP Sub-protocol da janela Statistics do CommView.**

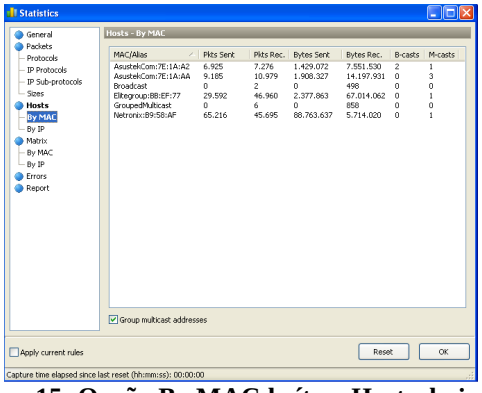


**Figura 15: Opção By MACdo ítem Hosts da janela Statistics do CommView.**

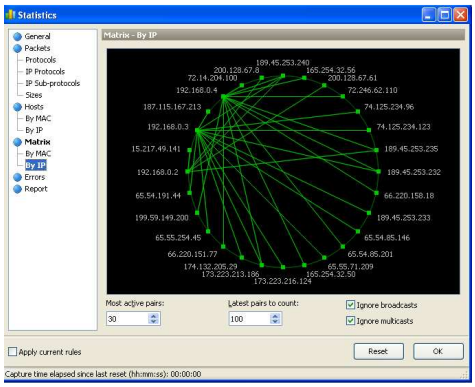


**Figura 16: Opção By IP do ítem Matrix da janela Statistics do CommView.**

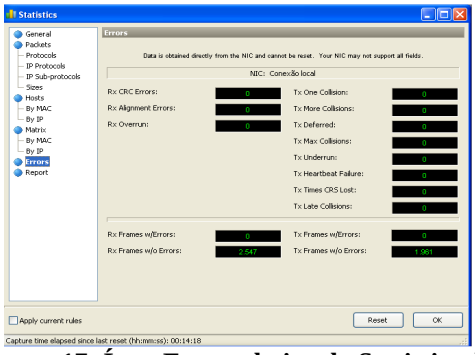


**Figura 17: Ítem Errors da janela Statistics do CommView.**

### *C. Tcpdump*

O Tcpdump, por ser uma ferramenta que funciona através de linha de comando, não oferece a geração de estatísticas.

### *D. Wireshark*

O *Summary* apresenta informações gerais sobre os dados da captura, como por exemplo, o tamanho em bytes da captura, o tempo quando o primeiro e o último pacote foram capturados, qual interface de rede utilizada, se foi feito o uso de filtros e o total de pacotes capturados. A Figura 18exibe a janela do *Summary* do *Wireshark*.


**Figura 18: Janela do Summary do Wireshark**

A opção *Protocol Hierarchy* apresenta uma janela com a árvore de todos os protocolos capturados. Além de possuir dados e valores estatísticos, como por exemplo, o nome do protocolo, a porcentagem de pacotes correspondente em relação a todos os pacotes na captura, o número absoluto de pacotes e a largura de banda utilizada por cada protocolo. A janela da opção *Protocol Hierarchy*, é exibida na Figura 19.

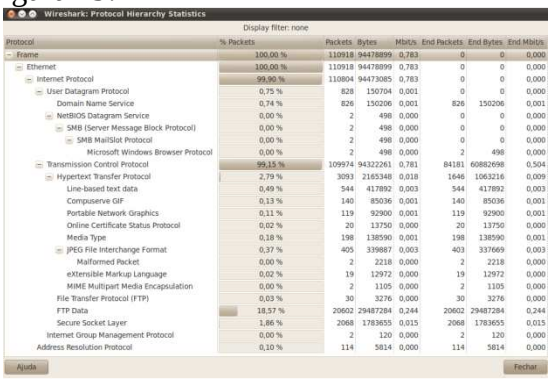


**Figura 19: janela da opção Protocol Hierarchy do Wireshark**

A opção *Conversation* apresenta o tráfego entre dois pontos específicos, cada linha na lista mostra os valores estatísticos de cada conversa.

Em uma conversa entre endereços IP, por exemplo, contêm informações dos pacotes enviados e recebidos entre eles. Informações como, quantidade de pacotes, o seu tamanho em bytes e o tempo em segundos entre o início da captura e no início da conversa. Essa janela é atualizada com frequência e é exibida na Figura 20.

A opção *Endpoints* apresenta todos os pontos finais do tráfego da rede representado por endereços IP, assim como, a quantidade de pacotes e seu tamanho em bytes.

A opção *IO Graphs* apresenta um gráfico de todo o fluxo de pacotes trafegados na rede. É possível realizar configurações de visualização, como por exemplo, definir até cinco gráficos com cores e filtros diferentes, alterar o estilo de exibição e a escala de tempo e a unidade de medida. Além disso, é possivel salvar o gráfico como uma imagem.

A janela do *IO Graphs* é exibida na Figura 21.

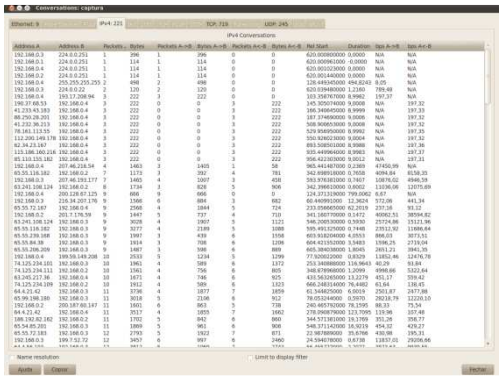


**Figura 20: janela da opção Conversations do Wireshark**

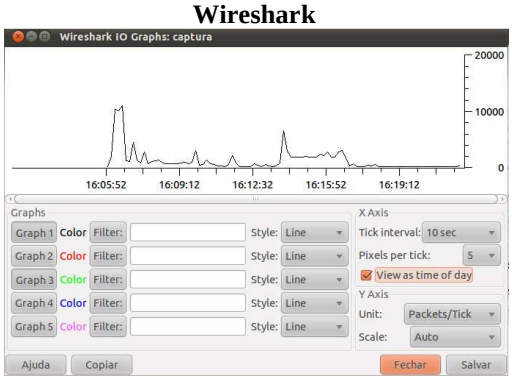


**Figura 21: Janela da opção IO Graphs do Wireshark.**

## 7. Análise Comparativa

O presente estudo mostra diversas funcionalidades de cada ferramenta. A Tabela 10 apresenta a comparação dessas funcionalidades.

A ferramenta *Capsa Network Analyser*, apresenta qualidade em sua interface gráfica por ser semelhante aos softwares do pacote Microsoft Office 2007, facilitando e tornando intuitivo o seu uso. O usuário pode facilmente mudar de uma estatística geral para os detalhes de um nó de rede específico através de um clique. Possibilita a configuração de regras de alarmes e suas notificações. Seu uso é exclusivo da plataforma Windows.

O *CommView* é composto por uma interface gráfica simples e bastante amigável composta por seis guias que permitem a visualização dos dados. Possibilita a configuração de alarmes, importação e exportação de arquivos capturados em diversos formatos, relatórios HTML, reconstrução de seções TCP, geração de pacotes personalizados e monitoramento remoto. Assim como o *Capsa*

*NetworkAnalyzer*, é uma ferramenta para o ambiente Windows.

O *Tcpdump* é uma ferramenta que atua através de linha de comando, portanto não possui recursos gráficos que facilitam a sua execução. Porém exige menos processamento da máquina ao ser submetida a execução evitando a perda de pacote. É uma ferramenta livre, gratuita e própria para ambiente Linux. Todavia, apesar de operar em linha de comando, seus comandos e a sintaxe dos filtros são simples e fáceis de utilizar. A sua utilização em conjunto com outras ferramentas analisadoras de pacotes se torna eficaz, por possibilitar uma maior integridade nos pacotes capturados.

O *Wireshark* é uma ferramenta livre, multiplataforma, gratuita, que opera tanto em ambiente Linux como em ambiente Windows. Possui uma interface gráfica bastante simples e intuitiva. A visualização dos pacotes capturados é baseada em um sistema de cores, no qual cada cor corresponde a um protocolo diferente, recurso que não foi encontrado nas outras ferramentas. Com a ferramenta *Wireshark*, a empresa evitará custos com a compra de licença, e poderá utilizar de funcionalidades como a decodificação de pacotes, a montagem de sessões TCP, diagrama de toda conexão TCP, entre outros. Possibilita um completo e eficiente troubleshooting dos problemas de rede, dos mais básicos até os mais avançados. Para isso necessita-se de um grande entendimento dos protocolos envolvidos na comunicação dos dados entre os dispositivos, tais como computadores, switches e roteadores.

## 8. Considerações Finais.

Tendo em vista as características das ferramentas proprietárias, conclui-se que dentre as apresentadas, a ferramenta que obteve melhor destaque em termos de execução, funcionalidade e usabilidade, foi a Capsa *Network Analyzer*. Esta fornece ao usuário maior facilidade em relação à compreensão dos gráficos, estatísticas e conteúdo dos pacotes trafegados na rede, em comparação com o *CommView*.

Ao observar as características das ferramentas livres, conclui-se que o *Tcpdump*, apesar de operar em linha de comando, é capaz de capturar os pacotes de rede com maior integridade, evitando possíveis perdas desses pacotes. Entretanto, o *Wireshark*, por possuir interface gráfica, facilita a visualização e entendimento dos pacotes de rede capturados através de gráficos. Assim, para obter uma análise mais precisa, sugere-se a utilização em conjunto dessas duas ferramentas.

Notou-se que as funcionalidades disponíveis nas ferramentas livres podem atender com eficácia a realização das atividades de captura e análise de pacotes. Quanto às ferramentas proprietárias, que necessitam de licença, características comuns às gratuitas foram observadas, entretanto foi observada, também, a presença de recursos que facilitam a atividade de análise dos pacotes, como por exemplo, a geração de relatórios de todo o tráfego passado pela rede.

Diante disso, considerando as reais necessidades da empresa, a escolha de uma ferramenta deve proporcionar a melhor relação custo x benefício.

## Referências

BANERJEE, USHA; VASHISHTHA, ASHUTOSH; SAXENA, MUKUL. **Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection**.In: InternationalJournalof Computer Applications. v. 6, n. 7, 2010.

COMER, DOUGLAS E. **Redes de Computadores e a Internet - Abrange transmissão de dados, ligações inter-redes, web e aplicações**. 4. ed. Rio de Janeiro: Bookman, 2007

CORRÊA, JORGE L.; PROTO, ANDRÉ; CANSIAN, ADRIANO M. **Modelo de armazenamento de fluxos de rede para análises de tráfego e de segurança**. In: VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Anais. 2008. Disponível em: <http://sbseg2008.inf.ufrgs.br/anais/data/pdf

| Funcionalidades | *Capsa Network Analyzer* | *CommView* | *Tcpdump* | *Wireshark* |
|---|---|---|---|---|
| Plataforma Windows | Sim | Sim | Não | Sim |
| Plataforma Linux | Não | Não | Sim | Sim |
| Captura de pacotes | Sim | Sim | Sim | Sim |
| Armazenamento dos pacotes | Sim | Sim | Sim | Sim |
| Exibição dos pacotes | Sim | Sim | Sim | Sim |
| Utilização de filtragem de pacotes | Sim | Sim | Sim | Sim |
| Exibição da duração da captura | Sim | Sim | Não | Sim |
| Dados da utilização da banda utilizada | Sim | Sim | Não | Sim |
| Contagem de pacotes | Sim | Sim | Sim | Sim |
| Estatística dos protocolos | Sim | Sim | Não | Sim |
| Estatísticas dos endereços MAC | Sim | Sim | Não | Sim |
| Estatísticas dos endereços IP | Sim | Sim | Não | Sim |
| Estatísticas dos endereços MAC | Sim | Sim | Não | Sim |
| Estatísticas das conversas entre endereços MAC e IP | Sim | Sim | Não | Sim |
| Estatísticas das conversas TCP e UDP | Sim | Sim | Não | Sim |
| Geração de gráficos | Sim | Não | Não | Sim |
| Matriz do tráfego da rede | Sim | Sim | Não | Não |
| Geração de logs | Sim | Sim | Não | Não |
| Alarmes | Sim | Sim | Não | Não |
| Preço | U$999,00 | U$ 499,00 | R$0,00 | R$0,00 |

**Tabela 10. Comparativo das Funcionalidades das Ferramentas**

/st02_03_artigo.pdf >. Acesso em 20 de agosto de 2011.

CERT.br – **Sobre o CERT.br**. Disponível em: < http://www.cert.br/sobre >. Acesso em 27 de ago. 2011.

KUROSE, JAMES F.; ROSS, KEITH W. **Redes de Computadores e a Internet: Uma abordagem top-down**. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

MARCELLA, ALBERT J.; MENENDEZ, D. **Cyber Forensics – A Field Manual for Colleting, Examining, and Preserving Evidence of Computer Crimes**.2. ed. Boca Raton: AuerbachPublication, 2008.

NBR ISO/IEC 27002. **Tecnologia da informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2005.

NAKAMURA, EMILIO T.; GEUS, PAULO L. **Segurança de Redes em Ambientes Coorporativos** – Fundamentos, Técnicas, Tecnologias, Estratégias. São Paulo: Novatec, 2007.

SANDERS C. **Practical Packet Analysis - Using Wireshark to Solve Real- World Network Problems**.São Francisco: No Starch Press, 2007

SILVA, GILSON MARQUES DA, LORENS, EVANDRO MÁRIO.**Extração e Análise de Dados em Memória na Perícia Forense Computacional**. In: Proceeeding of the Fourth International Conference of Forensic Computer Science (ICoFCS'2009), p. 29-36, Natal, 2009.

www.cert.br

www.colasoft.com/

www.tamos.com/

www.tcpdump.org/

www.wireshark.org/