SniffAndLearn: Uma Ferramenta para Suporte ao Ensino de Redes de Computadores Através do Monitoramento de Pacotes

João Luiz C. Carvalho, Daniel G. Costa

Curso de Engenharia de Computação
Departamento de Tecnologia
Universidade Estadual de Feira de Santana (UEFS)

{joaoluiz,danielgcosta}@ecomp.uefs.br

Abstract. *The conceiving of computer networks and the Internet has provided a revolution in all areas of knowledge. However, these communication structures have a high complexity, demanding a significant effort by students and professionals in the understanding of the operating mechanism related with computer networks, even partially. To support the teaching and learning of Internet protocols, a tool intended to assist the study of the architectures and patterns used on the Internet was developed, based on packets monitoring,. Identifying communications and presenting additional information, SniffAndLearn intend to aid in computer network teaching.*

Resumo. *A concepção das redes de computadores e da Internet proporcionou uma revolução em todas as áreas do conhecimento. Contudo, essas estruturas de comunicação bastante complexas vêm demandando um significativo esforço por parte de estudantes e profissionais para que seu mecanismo operacional seja compreendido, mesmo que parcialmente. Para dar apoio ao ensino e aprendizagem de protocolos da Internet, foi desenvolvida uma ferramenta que pretende auxiliar, através do processo de monitoramento de pacotes, o estudo da arquitetura e dos padrões utilizados na Internet. Identificando comunicações e apresentando informações complementares aos usuários, SniffAndLearn pretende ser um recuso didático complementar no ensino de redes de computadores.*

1. Introdução

A Internet é um ambiente de comunicação rico em heterogeneidade. Formada por uma infra-estrutura não linear e interconectando redes de computadores domésticas, corporativas e governamentais, a Internet foi concebida para permitir a comunicação entre grupos de pessoas de todo o mundo [Tanembaum, 2003]. Nos últimos anos, essa rede mundial de computadores se tornou um recurso essencial para o homem moderno.

A grande demanda por comunicação na Internet vem provocando uma corrida por equipamentos e ferramentas que provêem alta velocidade e confiabilidade de comunicação. Hoje, a Internet é uma rede diversificada, com largura de banda relativamente grande, e que suporta diversos tipos de serviço, desde a navegação web

através de um computador tradicional até a telefonia celular, incluindo também sistemas computacionais em automóveis e equipamentos de sensoriamento ambiental, apenas para citar alguns exemplos [Kurose e Ross, 2006].

Perante a diversidade de serviços disponíveis na Internet, se tornou necessária a utilização de protocolos para o estabelecimento de padrões de comunicação em meio a tecnologias e demandas distintas. Atualmente, uma pilha de protocolos compõe uma parte essencial da Internet e do estudo de redes de computadores. Tipicamente, cada serviço da Internet utiliza um ou mais protocolos da pilha de protocolos Internet, também chamada de arquitetura TCP/IP, a exemplo do HTTP (Hypertext Transfer Protocol) para navegação web [Fielding et al., 1999], DNS (Domain Name System) para resolução de nomes de domínio [Mockapetris, 1987], TCP (Transmission Control Protocol) para comunicação fim-a-fim [DARPA(a), 1981], entre muitos outros. Atualmente, estes serviços podem ser utilizados concorrentemente em qualquer computador ou rede de computadores, o que implica em um tráfego de diferentes conteúdos em uma única arquitetura de rede.

Uma das formas de se analisar o funcionamento de uma rede de computadores é através de uma ferramenta de monitoramento de pacotes, ou *sniffer* [Comer, 1998]. Essa ferramenta captura todos os pacotes que chegam à interface de rede da máquina onde o monitoramento está sendo realizado [Hunt, 2002]. Um *sniffer* é útil para examinar problemas de rede, detectar falhas de segurança e depurar implementações de protocolos, uma vez que muitos detalhes das comunicações e dos protocolos podem ser obtidos com ferramentas desse tipo, mesmo que indiretamente.

Verifica-se muitas vezes que nas ferramentas atuais de monitoramento, o resultado de uma captura de pacotes é apresentado ao usuário de forma pouco intuitiva. Os critérios de análise presentes nos *sniffers* convencionais são simplesmente de identificação do conteúdo dos pacotes e disponibilização de dados estatísticos, não existindo uma análise funcional das comunicações realizadas durante a captura. Alterando a forma como as informações são apresentadas, aliada a diversidade de informações disponíveis através de procedimentos de captura de pacotes, é possível utilizar *sniffers* para auxiliar estudantes a aprender sobre detalhes internos de protocolos de rede, criando-se assim um recurso didático complementar aos meios tradicionais de ensino.

Nesse contexto, foi desenvolvida uma ferramenta para dar suporte ao ensino de redes de computadores através da análise de pacotes capturados em procedimentos de *sniffing*, utilizando para isso recursos visuais para a apresentação de informações sobre os protocolos e as comunicações, recursos esses não presentes em ferramentas tradicionais de monitoramento de pacotes. Além disso, são apresentadas informações textuais complementares associadas a detalhes dos protocolos e das comunicações. Por fim, essa ferramenta, batizada de SniffAndLearn, permite a identificação automática de comunicações, que passam a ser representadas visualmente na forma como estão presentes na maioria dos livros didáticos da área.

A utilização de *sniffers* para suporte ao ensino de redes de computadores não é uma novidade, embora seja uma abordagem recente. Em [Fernadez e Martinez, 2009], é apresentada uma ferramenta que utiliza as informações obtidas em pacotes capturados em procedimentos de *sniffing* para auxiliar no estudo de redes de computadores. SniffAndLearn possui uma abordagem semelhante, porém traz o recurso adicional de

identificação automática de comunicações, que passam a ser visualizadas de forma mais intuitiva e próxima das representações presentes em grande parte da bibliografia de redes de computadores. A utilização de grafos para representação de comunicações também é uma abordagem inovadora da ferramenta desenvolvida.

Esse artigo está organizado da seguinte forma. Na segunda seção são apresentados alguns conceitos relacionados ao suporte ao ensino de redes de computadores. Na terceira seção é apresentada a ferramenta desenvolvida, juntamente com descrições sobre a especificação e sua implementação. Já na quarta seção são apresentados os testes e resultados da utilização prática da ferramenta SniffAndLearn. Por fim, encontram-se as considerações finais do trabalho e as referências bibliográficas.

2. Suporte ao Ensino de Redes de Computadores

O avanço da tecnologia e a introdução do computador no ambiente doméstico e educacional provocaram uma revolução nos métodos e concepções de ensino e aprendizagem [Valente, 1993]. Atualmente, a informática está sendo amplamente lecionada nos ensinos fundamental e médio, e também em cursos superiores, mesmos aqueles que não são de áreas afins à computação. Essa mudança no processo de ensino-aprendizagem se deve não só pelo fato do computador ser um artefato imprescindível no cotidiano da sociedade, mas por este se tratar de um recurso tecnológico com grande potencial pedagógico para os professores [Mendes et al., 2007].

A utilização do computador no processo de ensino-aprendizagem pode se dar de formas diferentes, a depender do contexto. Em [Valente, 1993], a utilização do computador na educação está classificada em duas finalidades: (i) ensino de computação, (ii) ensino através do computador. Enquanto no segundo o computador é utilizado apenas como um recurso didático multimídia que promove o aprendizado dinâmico e atrativo, no ensino de computação, ou "*computer literacy*", o computador não é meramente uma ferramenta de facilitação da aprendizagem, mas também o objeto de estudo.

Em ambos os casos anteriores, o computador por si só não é um recurso didático, pois o mesmo não foi concebido para ser, puramente, uma solução pedagógica. Necessita-se, então, que o computador disponha de um software educacional, que é responsável pela interação do estudante com a máquina. Um software educacional ou software educativo é “todo sistema que tem o objetivo de melhorar o processo ensino-aprendizagem de um conteúdo ou assunto educacional” [Mendes et al., 2007].

Em [Taylor, 1980], os softwares educativos são classificados em basicamente três tipos: o tutor, software que “ensina” o aluno; o tutorado, que dá ao aluno o papel de instruir o computador; e a ferramenta, software com o qual o aluno apenas manipula a informação. Valente (1993, p. 13) vai ao encontro da opinião de Taylor quando cita que “o computador pode ser utilizado como ferramenta educacional”, em que o aprendizado ocorre através da execução de uma tarefa por intermédio do computador. O mesmo autor inclui como tais tarefas a pesquisa de banco de dados, resolução de problemas utilizando linguagem de programação e o uso de rede de computadores como alguns exemplos de ensino-aprendizagem em computação com o auxílio do computador.

Entretanto, até mesmo na área de computação existe carência de ferramentas educacionais de apoio ao ensino-aprendizagem. A utilização do computador como um

recurso didático é bem vindo nessa área, principalmente porque ele mesmo é o objeto de estudo. Por exemplo, a própria infra-estrutura de rede na qual o computador está inserido pode ser aproveitada para criar uma plataforma didática que interaja o aluno com a rede de computadores. Neste mesmo exemplo, alguns princípios podem ser abordados, como as tecnologias das redes de computadores, os padrões de comunicação da Internet e alguns conceitos de concorrência e conectividade em computação, apenas para citar alguns exemplos.

O monitoramento de pacotes pode também ser utilizado como um potencial recurso de suporte ao ensino, pois representa em tempo real o funcionamento de uma rede de computadores, apresenta detalhes internos de cada protocolo e é fiel quanto ao conteúdo dos pacotes. SniffAndLearn está diretamente fundamentada nesse princípio.

3. A Ferramenta SniffAndLearn

O SniffAndLearn é, antes de tudo, um *sniffer* que possui os recursos tradicionais de um analisador de protocolos convencional. Essa ferramenta disponibiliza informações dos pacotes capturados instantaneamente para o usuário, porém são os recursos adicionais de análise das comunicações presentes nessa ferramenta que se destacam em relação a outros *sniffers*.

A ferramenta SniffAndLearn apresenta um novo enfoque para visualização da troca de mensagens entre os computadores, representando as informações de forma intuitiva. A ferramenta mantém a fidelidade das informações capturadas, mas as representam de maneira mais "sutil" para o usuário, analisando e ilustrando cada parte da informação. Para possibilitar essas novas análises, um módulo de interpretação deve ser criado para cada protocolo. Na versão inicial da ferramenta, foram criados módulos para os protocolos IP (Internet Protocol) [DARPA(b), 1981], TCP, UDP (User Datagram Protocol) [Postel, 1980], ARP (Address Resolution Protocol) [Plummer, 1982], ICMP (Internet Control Message Protocol) [Postel, 1981], HTTP e DNS.

O escopo da ferramenta se define em quatro componentes: captura, processamento do conteúdo dos pacotes, análise das comunicações e interface com o usuário. Esses componentes definem um fluxo de informações, desde a captura de pacotes até a interface com o usuário. A ferramenta foi desenvolvida de modo que seus componentes estivessem pouco acoplados, para que novos recursos pudessem ser facilmente acrescentados futuramente, como o processamento do conteúdo de novos protocolos, por exemplo.

A estratégia de desenvolvimento do SniffAndLearn consistiu em uma parte inicial, referente a especificação do sistema através da definição dos requisitos e dos rascunhos da interface com usuário, e em uma segunda parte, que foi o projeto e desenvolvimento efetivo do software. A primeira parte teve grande importância porque o SniffAndLearn tem como ponto chave a interação com o usuário, e, por isso, os rascunhos da interface gráfica foram pontos fundamentais da especificação.Na etapa de implementação foi utilizado o processo de desenvolvimento de software incremental. Esse processo consiste em identificar as funções mais importantes e em seguida definir uma série de estágios de entrega, em que cada entrega possui uma funcionalidade adicional em relação à anterior [Sommerville, 2003]. No desenvolvimento incremental estão inseridas as etapas de levantamento de requisitos, projeto da arquitetura do

sistema, desenvolvimento, validação e integração dos incrementos e validação do sistema final como um todo.

A linguagem de programação utilizada para desenvolver o *SniffAndLearn* foi Java [Deitel, 2005]] na sua versão 1.6, devido a grande quantidade de recursos que essa linguagem possui, a existência de muitas bibliotecas *open source*, e também pela sua independência de plataforma. A captura dos pacotes que chegam a uma interface de rede do computador é feita por meio do JPcap [JPCAP, 2007], uma biblioteca *open source* desenvolvida em Java para operações de *sniffing*, contendo recursos para capturar e enviar pacotes pela rede, salvar pacotes capturados em arquivo e adicionar filtros à captura. O JPcap requer uma biblioteca externa ao Java para poder operar corretamente, devido às limitações da linguagem Java em relação ao acesso a alguns recursos de hardware. Em sistemas operacionais Linux, essa biblioteca é a libpcap [Libpcap, 2010], no Windows a biblioteca é Winpcap [Varenni, 2010] e no Mac OS é a biblioteca Xcode [Apple Inc., 2010].

A ferramenta SniffAndLearn pode ser obtida gratuitamente através do endereço da web http://www.ecomp.uefs.br/~danielgcosta/programas/sniffandlearn/index.php. Nesse endereço eletrônico também se encontra um vídeo apresentado a ferramenta em execução.

4. Testes e Resultados

Após o desenvolvimento da ferramenta, verificou-se a necessidade da realização de testes que pudessem atestar a ausência de falhas de implementação e verificar a adequação das suas funcionalidades em relação aos objetivos iniciais. Essas duas situações foram tratadas em abordagens diferentes.

Utilizando os requisitos definidos para a ferramenta, diversos casos de teste foram desenvolvidos para verificar o produto final. Esses testes foram realizados na rede da Universidade Estadual de Feira de Santana, devido, sobretudo, ao tráfego variado gerado por aplicações em operação nessa rede. A metodologia do caso de teste "principal" foi iniciar, a partir do computador onde a ferramenta SniffAndLearn está em execução, uma verificação de acessibilidade através do programa "ping" [Hunt, 2002] e um acesso a uma página web (endereço www.google.com). Os principais eventos relacionados a esse caso de teste específico serão apresentados a seguir.

O botão "Iniciar Captura" na janela principal da ferramenta dá início ao processo de captura de pacotes. Durante esse processo, é iniciado o acesso à página "www.google.com.br" e realizado o teste de acessibilidade a um endereço interno da rede. Nesse momento, os pacotes capturados são instantaneamente exibidos na janela principal, conforme apresenta a Figura 1. O usuário pode parar o processo a qualquer momento clicando no botão "Parar Captura".

Ao parar a captura, pode-se visualizar o conteúdo de um pacote capturado clicando sobre o mesmo na janela principal. Uma nova janela é aberta, mostrando os cabeçalhos e os dados de um pacote. A Figura 2 apresenta a janela com o conteúdo de um pacote ICMP, resultado do teste de acessibilidade iniciado com o programa "ping".

Pode-se observar nessa Figura que os cabeçalhos das mensagens IP e ICMP são mostrados em abas diferentes, podendo assim o usuário verificar as informações nas diversas abstrações lógicas presentes nas redes de computadores modernas. Essa forma

de visualização não está presente nos *sniffers* tradicionais, estando mais próximo das representações presentes em livros didáticos da área.

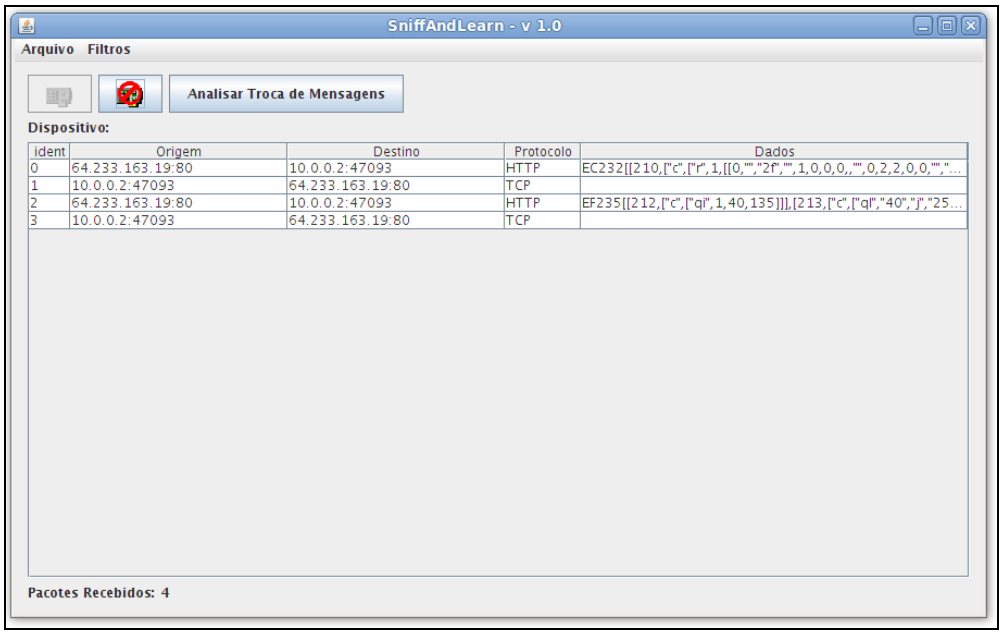

Figura 1. Tela principal da ferramenta durante uma captura.

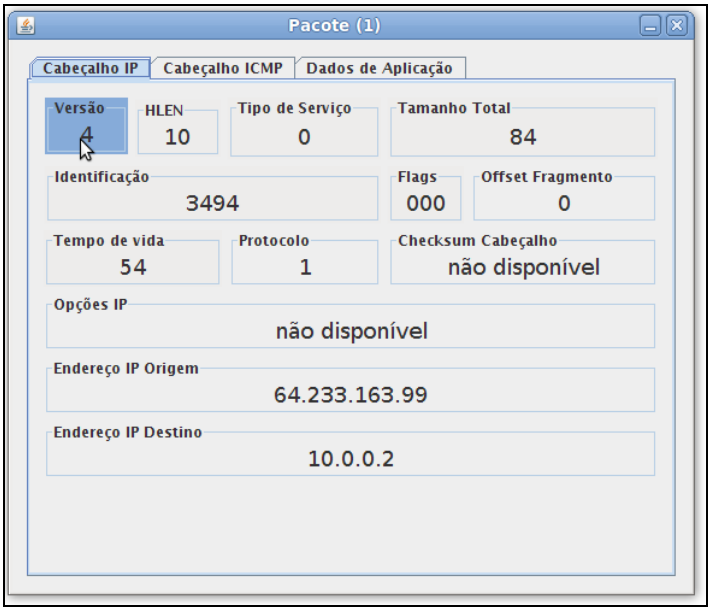

Figura 2. Visualização detalhada e segmentada de informações de um pacote ICMP.

Ao clicar sobre um dos campos do cabeçalho, de qualquer um dos protocolos relacionados a esse pacote específico, o usuário obtém um texto explicativo sobre esse campo. Na Figura 3 é apresentada uma tela com uma informação explicativa sobre o campo versão do pacote IP.

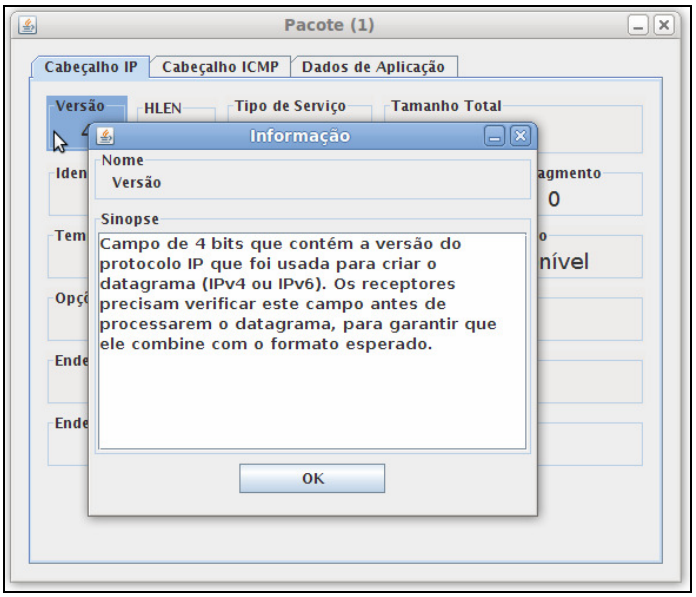

Figura 3. Texto explicativo referente a um campo de um protocolo.

A página "www.google.com" acessada pelo usuário gerou um tráfego DNS. A mensagem de consulta DNS é apresentada na Figura 4(a), que mostra o cabeçalho e a seção de pergunta da mensagem desse protocolo. Os pacotes da conexão HTTP com o servidor da página web foram também capturados, sendo um deles apresentado na Figura 4(b), que exibe a linha de método (POST), alguns parâmetros e o corpo da mensagem.

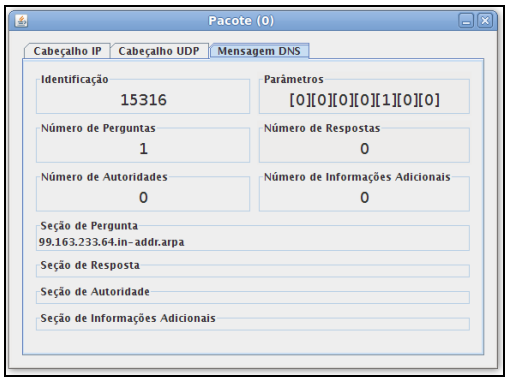

Figura 4(a). Campos referentes a uma mensagem de consulta DNS.

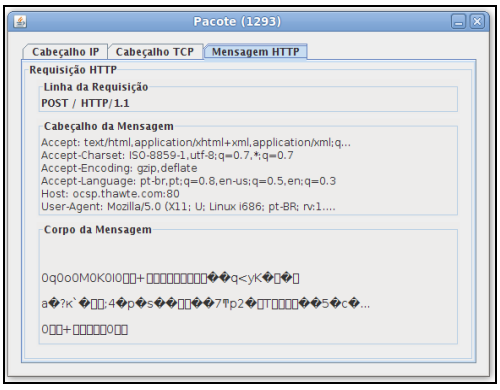

Figura 4(b). Mensagem de requisição HTTP.

As comunicações realizadas durante a captura são processadas quando o usuário aperta o botão "Analisar Troca de Mensagens.". Nesse momento, uma janela é aberta para o usuário com todas as comunicações realizadas, mostrando as extremidades e a quantidade de pacotes trocados. A partir dessa janela o usuário pode visualizar o grafo com todas as extremidades identificadas na captura, visualizar um "log" das comunicações ou analisar uma comunicação individualmente.

A representação em grafo oferece uma forma inovadora e bastante intuitiva de identificação de comunicações. A Figura 5 apresenta um exemplo de representação das

comunicações em forma de grafo, onde o nó central do grafo está em comunicação com todos os outros nós. Caso a ferramenta SniffAndLearn seja executada em um computador onde passem comunicações de outras máquinas, mais de um grafo será apresentado nesse tipo de visualização.

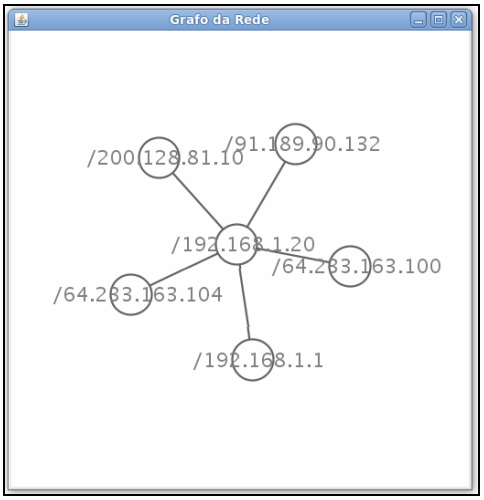

Figura 5. Grafo representando as comunicações descobertas pela ferramenta.

Na análise individual de uma comunicação, o usuário visualiza um esquema de troca de mensagens semelhante a um diagrama de sequência da linguagem UML (Unified Modeling Language) [Fowler, 2004], sendo essa uma abordagem comum em livros da área de redes de computadores. Cada extremidade é exibida como um endereço IP, e os pacotes trocados entre eles são separados por protocolo, em abas. Em cada aba de protocolo, os pacotes são vistos como setas entre as extremidades, organizadas sequencialmente. Todos os pacotes contêm um rótulo que informa qual o tipo de seu conteúdo. A Figura 6 apresenta uma parte da troca de mensagens no acesso à página web considerada nesse caso de teste. Nessa Figura, cada aba apresenta a troca de mensagens respectiva à camada lógica de rede correspondente.

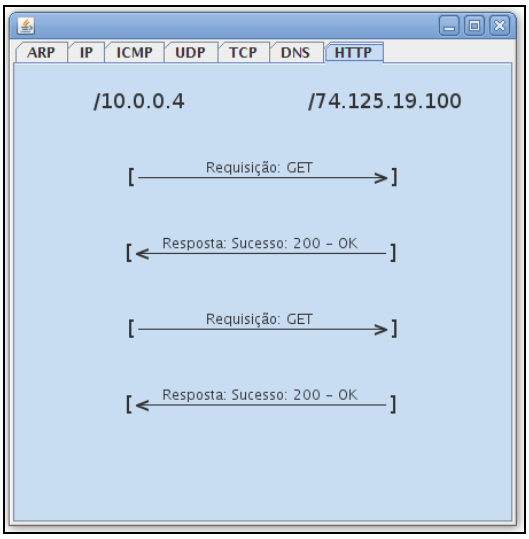

Figura 6. Exemplo de uma troca de mensagens HTTP.

O passo seguinte dos testes consiste na aplicação da ferramenta em disciplinas relacionadas às redes de computadores, como um recurso didático auxiliar. Após a aplicação desses testes, a avaliação final dos alunos nas disciplinas será comparada com semestres anteriores, buscando encontrar alguma relação de melhoria com a utilização da ferramenta. Essa fase dos testes está ainda em andamento, visto que são necessários alguns semestres para que análises estatísticas sejam feitas com mais segurança, minimizando discrepâncias naturais entre o rendimento de turmas diferentes.

5. Considerações Finais

O monitoramento de pacotes é, sem dúvida, uma das formas de se compreender os padrões utilizados na Internet. Contudo, esse recurso não tem sido bem empregado no processo de ensino de redes de computadores, devido, sobretudo, às limitações na forma de representação das informações sobre os protocolos e as comunicações. Os detalhes técnicos apresentados em um *sniffer* convencional dificultam a compreensão das informações adquiridas, por parte dos usuários.

O SniffAndLearn se apresenta como uma ferramenta inovadora, se destacando dos demais *sniffers* por oferecer um enfoque maior na interpretação dos pacotes e das comunicações. Esse aspecto é potencialmente vantajoso se sua utilização for inserida no processo de ensino e aprendizagem de redes de computadores, uma vez que os alunos acessam de forma mais intuitiva dados de comunicações reais. A partir dessas novas representações, analogias e comparações entre o conteúdo presente em livros e a análise de comunicações reais podem trazer diversos benefícios a esse processo de aprendizagem.

A versão atual da ferramenta SniffAndLearn possui os aspectos propostos inicialmente neste trabalho, que são a reprodução gráfica das comunicações em rede e a representação intuitiva dos dados da captura, suportando a maioria dos protocolos mais utilizados na Internet. Esses recursos colocam a ferramenta em posição de destaque como um recurso didático em disciplinas e cursos de redes de computadores.

Trabalhos futuros estarão focados na verificação prática dessa ferramenta em ambientes reais de ensino. Embora seja esperado diversos benefícios da utilização didática do SniffAndLearn, essa expectativa ainda não foi verificada na prática. Para endereçar essa questão, deverão ser realizados testes com usuários finais, coletando opiniões e sensações através de questionários, por exemplo.

Adicionalmente, trabalhos futuros estarão relacionados com a agregação de novos protocolos ao SniffAndLearn, uma vez que um dos objetivos da ferramenta é possibilitar a expansão do suporte aos padrões da Internet, e com o aperfeiçoamento dos recursos de interação com o usuário, adicionando recursos multimídia, como sons e animações.

Referências Bibliográficas

Apple Inc. (2010). “Tools - XCode. Developer Connection”. http://developer.apple.com/tools/xcode/. Acessado em 09 de Janeiro.

Comer, E. (1998). Interligação em Redes com TCP/IP. 3ª ed. Campus.

DARPA(a). (1981). “RFC 793: Transmission Control Protocol”. http://www.ietf.org/rfc/rfc793.txt. Acessado em 12 de Janeiro.

DARPA(b). (1981). “RFC 791: Internet Protocol”. http://www.ietf.org/rfc/rfc791.txt. Acessado em 13 de Janeiro.

Deitel, P. J. e Deitel, H. M. (2005). Java: Como Programar. 6ª ed. Prentice-Hall.

Fernandez, M. D. e Martinez, J. A. (2009). Intuitive learning of communication protocols by using a sniffer. In *Computer Applications in Engineering Education*.

Fielding, R., et al. (1999). “RFC 2616: Hypertext Transfer Protocol – HTTP/1.1”. http://www.ietf.org/rfc/rfc2616.txt. Acessado em 11 de Janeiro.

Fowler, M. (2004). UML Distilled: a Brief Guide to the Standard Object Modeling Language. 3ª ed. Addison-Wesley.

Hunt, C. (2002). TCP/IP Network Administration. 3ª ed. O´reilly.

JPcap. (2010). “Jpcap - a Java library for capturing and sending network packets”. http://netresearch.ics.uci.edu/kfujii/jpcap/doc/>. Acessado em 14 de Janeiro.

Kurose, J., Ross, K. (2006). Redes de Computadores e a Internet: uma abordagem top-down. 3ª ed. Pearson Addison Wesley.

Libpcap. (2010). TCPDUMP/LIBPCAP public repository. http://www.tcpdump.org/. Acessado em 09 de Janeiro.

Mendes, J. L., Carvalho, C. V. A. e Carvalho, J. V. (2007). Construfig3D: Uma Ferramenta Computacional para apoio ao ensino da Geometria Plana e Espacial. In *RENOTE. Revista Novas Tecnologias na Educação*, v. 5, p. 1/10.

Mockapetris, P. (1987). “RFC 1034: Domain Names – Concepts and Facilities”. http://www.ietf.org/rfc/rfc1034.txt. Acessado em 12 de Janeiro.

Plummer, David C. (1982). “RFC 826: An Ethernet Address Resolution Protocol”. http://www.ietf.org/rfc/rfc826.txt. Acessado em 15 de Janeiro.

Postel, J. (1980). “RFC 768: User Datagram Protocol”. http://www.ietf.org/rfc/rfc768.txt. Acessado em 12 de Janeiro.

Postel, J. (1981). “RFC 792: Internet Control Message Protocol”. http://www.ietf.org/rfc/rfc792.txt. Acessado em 13 de Janeiro.

Sommerville, I. (2003). Engenharia de Software. 6ª ed. Addison Wesley.

Tanembaum, A. S. (2003). Redes de Computadores. 4ª ed. Campus.

Taylor, R. P. (1980). “The Computer in the School: Tutor, Tool, Tutee”. New York: Teachers College Press.

Valente, J. A. (1993). “Diferentes Usos do Computador na Educação”. In: *Computadores e Conhecimento*. Campinas: Gráfica da Unicamp. p. 1-23.

Varenni, G. (2010). WinPcap: The Windows Packet Capture Library. <http://www.winpcap.org/>. Acessado em 09 de Janeiro.