

**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA SUL-
RIO-GRANDENSE - CÂMPUS PASSO FUNDO
CURSO DE TECNOLOGIA EM SISTEMAS PARA INTERNET**

LUIS FERNANDO POOTER

**ESTUDO SOBRE ASPECTOS DE SEGURANÇA NOS NAVEGADORES DE
INTERNET**

**PASSO FUNDO
2017**

LUIS FERNANDO POOTER

**ESTUDO SOBRE ASPECTOS DE SEGURANÇA NOS NAVEGADORES DE
INTERNET**

Projeto de pesquisa submetido ao Curso de Tecnologia em Sistemas para Internet do Instituto Federal Sul-Rio-Grandense, Câmpus Passo Fundo, como requisito parcial para a aprovação na disciplina de Projeto de Conclusão II (PC II).

Orientador: Me. Lisandro Lemos Machado

PASSO FUNDO

2017

LUIS FERNANDO POOTER

**ESTUDO SOBRE ASPECTOS DE SEGURANÇA NOS NAVEGADORES DE
INTERNET**

Trabalho de Conclusão de Curso aprovado em ____/____/____ como requisito parcial para a obtenção do título de Tecnólogo em Sistemas para Internet

Banca Examinadora:

Nome do Professor(a) Orientador(a)

Nome do Professor(a) Convidado(a)

Nome do Professor(a) Convidado(a)

Coordenação do Curso

PASSO FUNDO

2017

RESUMO

Esse trabalho tem como objetivo investigar a segurança dos principais navegadores de internet quanto a sua confidencialidade em operar as informações neles inseridas. No âmbito empresarial, a segurança dos dados e das informações que são gerados e circulam internamente, muitas vezes exigem caráter sigiloso. Atualmente a utilização da internet é praticamente inevitável, na qual é realizada por meio dos navegadores, onde o usuário, não tendo a segurança necessária e adequada, pode acabar fornecendo involuntariamente dados privados. Foi realizada uma comparação entre os principais navegadores, buscando verificar possíveis anormalidades entre eles no que se refere a sua segurança. Foram monitorados os fluxos de dados dos navegadores e realizada a comparação de dados enviados. Por fim, conclui-se que com estas metodologias de testes e comparações, o resultado obtido permite salientar possíveis navegadores de internet mais confiáveis para serem utilizados em âmbitos organizacionais.

Palavras-chave: Navegadores de internet. Segurança. Tráfego de rede. Confidencialidade.

ABSTRACT

This work aims to investigate the security of the main internet browsers regarding their confidentiality in operating the information inserted in them. At the business level, the security of data and information that is generated and circulated internally often requires secrecy. Currently the use of the internet is practically unavoidable, in which it is carried out through browsers, where the user, lacking the necessary and adequate security, may end up involuntarily supplying private data. A comparison was made between the main browsers, seeking to verify possible abnormalities between them in terms of their security. The data flows of the browsers were monitored and the data sent was compared. Finally, it is concluded that with these methodologies of tests and comparisons, the result obtained allows to highlight possible Internet browsers more reliable to be used in organizational environments.

Keywords: Internet browsers. Security. Network traffic. Confidentiality.

LISTA DE FIGURAS

Figura 1 - Market Share dos navegadores para desktops do mundo.....	19
Figura 2 - Market Share dos navegadores para desktops do mundo.....	19
Figura 3 - Estrutura de implementação	27
Figura 4 – Desktop Operating System Market Share	28
Figura 5 – Desktop Windows Version Market Share	28
Figura 6 – Exemplo de teste em andamento utilizando Browserscope	30
Figura 7 – Exemple resultado de teste utilizando HTML5 Test	31
Figura 8 – Complementos Internet Explorer desativados.....	34
Figura 9 – Extensões Chrome desativadas.....	34
Figura 10 – Extensões Firefox desativadas	35
Figura 11 – Extensões Opera desativadas	36
Figura 12 – Extensões Edge desativadas	36
Figura 13 – Seleção de Testes Utilizando Browserscope	37
Figura 14 – Página de teste Gmail	40
Figura 15 – Teste de envio de E-Mail e download de arquivo.....	40
Figura 16 – Página de autenticação do sistema Q-Acadêmico.....	41
Figura 17 – Página de autenticação do sistema Moodle.....	41
Figura 18 – Página de autenticação do E-Commerce Americanas	42
Figura 19 – Página de autenticação do E-Commerce Americanas	43
Figura 20 – Exemplo de captura de pacotes efetuado pelo Wireshark	44
Figura 21 – Teste de conexão sem navegação em um minuto com Internet Explorer	58
Figura 22 – Teste de conexão sem navegação em um minuto com Firefox	58
Figura 23 – Teste de conexão sem navegação em um minuto com Chrome	59
Figura 24 – Teste de conexão sem navegação em um minuto com Edge.....	59
Figura 25 – Teste de conexão sem navegação em um minuto com Opera	60
Figura 26 – Teste de conexão ao site Moodle em um minuto com Internet Explorer.....	61
Figura 27 – Teste de conexão ao site Moodle em um minuto com Firefox	61
Figura 28 – Teste de conexão ao site Moodle em um minuto com Chrome	62
Figura 29 – Teste de conexão ao site Moodle um minuto com Edge.....	62
Figura 30 – Teste de conexão ao site Moodle em um minuto com Opera	63

Figura 31 – Teste de conexão ao site Inf Passo Fundo em um minuto com Internet Explorer.....	63
Figura 32 – Teste de conexão ao site Inf Passo Fundo em um minuto com Firefox .	64
Figura 33 – Teste de conexão ao site Inf Passo Fundo em um minuto com Chrome	64
Figura 34 – Teste de conexão ao site Inf Passo Fundo em um minuto com Edge ...	65
Figura 35 – Teste de conexão ao site Inf Passo Fundo em um minuto com Opera ..	65
Figura 36 – Teste de conexão ao site Americanas em um minuto com Internet Explorer.....	66
Figura 37 – Teste de conexão ao site Americanas em um minuto com Firefox	66
Figura 38 – Teste de conexão ao site Americanas em um minuto com Chrome	67
Figura 39 – Teste de conexão ao site Americanas em um minuto com Edge.....	67
Figura 40 – Teste de conexão ao site Americanas em um minuto com Chrome	68
Figura 41 – Teste completo de conexão com Internet Explorer	69
Figura 42 – Teste completo de conexão com Firefox.....	69
Figura 43 – Teste completo de conexão com Chrome.....	70
Figura 44 – Teste completo de conexão com Edge	70
Figura 45 – Teste completo de conexão com Opera.....	71

LISTA DE TABELAS

Tabela 1 - Descrição dos testes realizados pelo Browserscope	14
Tabela 2 - Resultado do teste utilizando o Browserscope.....	45
Tabela 3 - Resultado do teste utilizando o HTML5 Test.....	46
Tabela 4 - Quantidade de pacotes capturados durante um minuto sem navegação.	48
Tabela 5 - Quantidade de pacotes capturados durante um minuto com navegação.	49
Tabela 6 - Quantidade de pacotes capturados durante um minuto com navegação.	50

SUMÁRIO

1.	INTRODUÇÃO.....	6
2.	SEGURANÇA DA INFORMAÇÃO	9
2.1.	CONFIDENCIALIDADE	10
2.2.	SEGURANÇA NAS ORGANIZAÇÕES	11
2.3.	FERRAMENTAS DE SEGURANÇA	13
2.3.1.	Kali Linux.....	13
2.3.2.	Browserscope	14
2.3.3.	Sniffers de Rede	16
3.	NAVEGADORES DE INTERNET	17
3.1.	O MERCADO DOS NAVEGADORES DE INTERNET.....	18
3.2.	CARACTERÍSTICAS DOS NAVEGADORES DE INTERNET	20
3.2.1.	Mozilla Firefox.....	21
3.2.2.	Internet Explorer.....	21
3.2.3.	Microsoft Edge	22
3.2.4.	Opera	22
3.2.5.	Google Chrome	22
3.3.	TRABALHOS CORRELATOS.....	22
4.	METODOLOGIA	26
4.1.	MÉTODOS E ARQUITETURA.....	26
4.2.	EQUIPAMENTOS E SISTEMAS.....	27
4.3.	FERRAMENTAS E SERVIÇOS	29
4.3.1.	BrowserScope.....	30
4.3.2.	HTML5 Test.....	31
4.3.3.	Wireshark.....	32
4.4.	AMBIENTE E METODOLOGIA DE TESTES.....	32
4.4.1.	Ajustes dos Navegadores de Internet.....	33
4.5.	METODOLOGIA DA REALIZAÇÃO DOS TESTES	37
4.5.1.	BrowserScope.....	37
4.5.2.	HTML5 Test.....	37
4.5.3.	Wireshark.....	38
5.	RESULTADOS OBTIDOS.....	45
5.1.	RESULTADOS DOS TESTES UTILIZANDO BROWERSCOPE	45

5.2. Resultados dos testes utilizando HTML5 Test.....	46
5.3. Resultados dos testes utilizando wireshark	47
5.3.1. Resultado: Teste de Minuto Sem Navegação	47
O número de pacotes transferidos durante a utilização de cada navegador em teste pode ser observado na coluna da direita desta tabela. Com apenas um teste, utilizando uma metodologia simples, sem navegação ou autenticação em sistemas fechados, onde apenas é inicializado o navegador, já é possível observar números elevados na comparação destes programas.....	48
5.3.2. Resultado: Teste de Minuto Com Navegação	48
5.3.3. Resultado: Teste Completo de Navegação	49
6. CONCLUSÃO	51
REFERÊNCIAS.....	56
APÊNDICE A - Resultado Teste de Minuto Sem Navegação	58
APÊNDICE B - Resultado Teste de Minuto Com Navegação	61
APÊNDICE C - Resultado Teste de Completo de Navegação	69

1. INTRODUÇÃO

Coordenar uma rede corporativa exige muitos desafios, é preciso ter e manter um controle das informações geradas com um alto nível de prioridade e sigilo. Muitas vezes o encarregado de uma rede empresarial, precisa escolher quais as melhores ferramentas para serem utilizadas dentro do domínio da organização pelos usuários, visando um nível de segurança mais amplo, onde as informações particulares inseridas nestas ferramentas de trabalho mantenham a sua política de privacidade.

É dever do coordenador da infraestrutura definir qual é a ferramenta mais confiável para o usuário da rede utilizar. Os navegadores de internet fazem parte destas ferramentas e são indispensáveis para acessar a internet, pois são o ponto de entrada para a rede mundial de computadores.

O administrador da rede tem um papel fundamental na empresa, atingindo diretamente os usuários colaboradores e ainda o funcionamento dos processos internos. A escolha por soluções melhores e mais seguras devem ser decididas com cautela. Existem inúmeras ferramentas e serviços no mercado com os mesmos objetivos, mas suas características diferem bastante umas das outras principalmente nas áreas de segurança da informação. O analista de rede deve decidir qual ferramenta seus usuários deverão utilizar, priorizando a segurança de cada um e a proteção das informações que os mesmos manipulam, deixando quesitos como desempenho e layout em segundo plano.

Por mais que os navegadores *web* sejam ferramentas comuns na vida *online* de cada indivíduo, poucas pessoas têm conhecimento da sua relevância ou se importam com a segurança de suas informações inseridas nesses programas. No ambiente empresarial até mesmo com programas tradicionais como os navegadores o administrador de rede precisa definir qual será o mais seguro a ser utilizado por seus usuários.

A escolha deste tema se deve a uma experiência profissional anterior com a oportunidade de fazer parte de uma equipe responsável pela infraestrutura da tecnologia da informação em uma grande empresa, sendo possível acompanhar os problemas diários que ocorrem em ambientes organizacionais. Mais próximo ao coordenador e responsável pela infraestrutura da rede, foi possível acompanhar os

problemas e decisões a serem tomadas para manter a rede empresarial segura, tal como as informações referentes à organização.

Durante esta experiência, o administrador da rede definiu um navegador web específico a ser utilizados por todos os usuários do domínio interno, tendo como permissão aos membros da equipe de TI, a exclusão de qualquer outro navegador ou software semelhante instalado no computador sem permissão. Estas decisões referentes aos navegadores motivou a realização de um estudo mais detalhado sobre o assunto para esclarecer dúvidas pertinentes a estas escolhas e definições.

Diante disso, o problema que impulsiona a presente pesquisa é a confidencialidade oferecida por estes navegadores de internet em manipular as informações pessoais de cada indivíduo. Assim, esta análise busca responder as seguintes perguntas: Existem navegadores mais confiáveis que outros? Os navegadores possuem diferenças em sua segurança quanto ao sigilo das informações? Existem outros destinos para as informações que inserimos nos navegadores?

Para responder estas questões, foram realizadas, pesquisas e testes utilizando os navegadores de internet como parte central deste estudo, o principal objetivo foi analisar a confiabilidade dos navegadores quanto a segurança das informações. Assim, foram estabelecidos critérios específicos a serem seguidos como etapas para chegar ao objetivo principal de forma organizada e correta.

É necessário primeiramente estudar os principais conceitos de segurança da informação, para ter uma compreensão melhor desta área da tecnologia. Determinar as características dos navegadores mais utilizados atualmente estudando as particularidades de cada um, pois são os softwares principais deste trabalho. Com isso, será possível estabelecer critérios de avaliação para determinar a confiabilidade dos navegadores a serem testados. Ainda, estudar e implementar métodos que possibilitem a realização de testes com navegadores. A última etapa deste processo é analisar a confiabilidade dos navegadores com base nos critérios de avaliação estabelecidos.

Diante do proposto trabalho, para que ocorra uma descrição detalhada e compreensível das etapas citadas, foi estabelecido uma divisão por capítulos deste modo é possível acompanhar gradativamente os processos realizados. O presente capítulo traz a introdução ao trabalho. O segundo capítulo apresenta os principais conceitos referentes ao tema proposto, dando enfoque na segurança da informação

e em ambientes corporativos. Em seguida, no terceiro capítulo, são apresentados e conceituados os navegadores de internet e ainda os trabalhos correlatos a esta pesquisa. No quarto capítulo, é descrita a metodologia implementada para atender ao propósito do trabalho e sua posterior análise. Para o quinto capítulo são apresentados os resultados obtidos através dos métodos propostos no capítulo anterior. Por fim, o sexto capítulo traz as conclusões e considerações finais da análise realizada.

2. SEGURANÇA DA INFORMAÇÃO

Difícilmente se chega ao fim de um dia sem que por uma única vez seja realizado uma troca de informação com alguém. Esta ação está mais presente e cresce exponencialmente com o uso das tecnologias atuais. Estes novos recursos aliados à internet possuem diversas funcionalidades, dentre as quais podem se destacar a de conectar seus usuários, para que os mesmos de uma maneira fácil e rápida consigam trocar informações.

Assim como em uma conversação presencial com uma pessoa, existem informações das quais o seu sigilo exige mais atenção, esta exigência também é válida quando esta troca de informação acontece dentro da internet, porém a dificuldade em manter o conteúdo em sigilo torna-se bem mais difícil. Quando passamos uma informação diretamente para um indivíduo, a exposição deste conteúdo para outros, somente acontecerá se o mesmo decidir revelar. Já em um ambiente virtual, a exposição desta informação não depende somente da confiança no receptor para mantê-la em segredo, pois ao inserir dados na internet, o risco de uma terceira parte ter acesso a este conteúdo se torna bem maior. A informação que pertence a determinados indivíduos, na internet, pode ser interceptada, roubada e até mesmo alterada se a rede não possuir seus devidos critérios de segurança.

Segundo define Moraes “a segurança da informação pode ser definida como um processo de proteger a informação do mau uso tanto acidental como intencional, por pessoas internas ou externas à organização, incluindo empregados, consultores e hackers”. (2010, p. 19). Este conceito de proteção esclarece e nos orienta quanto a importância da existência da segurança em torno das informações que manipulamos. É possível ainda, compreender que estamos vulneráveis a qualquer indivíduo, dentro ou fora, de uma rede privada, capaz de praticar atos que resultem no comprometimento das principais propriedades da segurança da informação.

Conforme Nakamura e Geus (2007, p.43) a confiabilidade, integridade e disponibilidade são propriedades indispensáveis para formar uma rede segura, são elas que vão garantir que apenas o usuário autorizado receba a informação enviada, sem alterações em seu conteúdo e totalmente protegida contra possíveis ameaças. Fontes (2016, p.11) conceitua estes três elementos fundamentais para a segurança da seguinte maneira:

“Disponibilidade: a informação deve estar acessível para o funcionamento da organização e para o alcance de seus objetivos e missão.

Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida.

Confidencialidade: a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização; para tanto, deve existir uma autorização prévia.”

Diante desses elementos, a presente pesquisa focará mais especificamente no conceito de confidencialidade, que será abordado a seguir.

2.1. CONFIDENCIALIDADE

A confidencialidade dos dados é o princípio da segurança que impulsiona esta pesquisa, pelo fato da sua importância, tanto para o usuário e quanto para a empresa, onde nas mãos erradas as informações privadas podem resultar em grandes prejuízos. Com isso, é totalmente indispensável um ambiente em que a segurança das informações ali inseridas seja considerada como prioridade a ser praticada.

Conforme Moraes “o princípio da confidencialidade é proteger a informação em sistemas, recursos e processos para que eles não possam ser acessados por pessoas não autorizadas” (2010, p. 28). Com isto é possível compreender que as diretrizes da confidencialidade abrangem diversos meios tecnológicos, neste caso abordado o software a ser analisado, onde este precisa obrigatoriamente manter em sigilo e segurança as informações que seus usuários manipulam internamente no programa.

A confidencialidade trata de preservar nossos dados pessoais na internet. Ao acessar uma página web em que é solicitado um dado pessoal, se ela apresentar um ícone de cadeado no canto do navegador de internet, isso representa que muitos processos são executados em segundo plano para manter a confidencialidade dos dados inseridos. O navegador inicia um processo de autenticação do site, enquanto este realiza o mesmo processo no navegador para verificar se o mesmo é autêntico ou se estamos autorizados a acessar a página web de acordo com a política de controle. O navegador então solicita à página web, uma chave de encriptação para codificar os dados e envia-los apenas no formato encriptado (Goodrich e Tamassia , 2013).

Este elemento fundamental que faz parte da segurança da informação possui uma importância tão grande que por vezes torna-se difícil de mensurar. Na tecnologia da informação existem inúmeras variáveis que influenciam diretamente nos resultados. Utilizar métricas para avaliar a confidencialidade de ferramentas e serviços referentes a tecnologia é possível, porém alguns empecilhos impedem uma análise mais detalhada e completa destes produtos. O acesso ao código fonte de determinados programas pode ser citado como um exemplo destas dificuldades. Não ter acesso ao código do sistema dificulta na realização de uma análise clara das métricas utilizadas pelos desenvolvedores na aplicação de seus sistemas.

Outro fator importante na hora de mensurar a confidencialidade de um produto, e que também possui um grau de dificuldade maior quando realizado, é acompanhar o tráfego de dados que os mesmos realizam durante seu funcionamento. Monitorar todo este fluxo de movimentação das informações exige cautela e um conhecimento avançado para que seja possível interpretar os resultados obtidos e tomar as decisões cabíveis.

Em organizações empresariais este acompanhamento do tráfego das informações internas é realizado a todo momento. Existe uma preocupação relevante no sentido de se ter conhecimento das informações que entram e, principalmente, saem da empresa. Sendo ainda capaz de obter informações como origem e destino destes dados que circulam na rede interna. É importante então que, quando da adoção de softwares, seja em ambiente empresarial quanto doméstico, se tenha atenção, dentre outros elementos, no aspecto da confidencialidade.

2.2. SEGURANÇA NAS ORGANIZAÇÕES

As informações que são geradas e manipuladas dentro de ambientes empresariais são recursos fundamentais para o negócio. Os dados contidos nestas informações podem ser fundamentais para o futuro da empresa podendo influenciar diretamente no seu rendimento, de forma positiva se for utilizado de maneira correta, ou trazendo grandes prejuízos se empregado de maneira equivocada.

Para Nakamura e Geus, (2007, p.49), “uma falha, uma comunicação com informações falsas ou um roubo ou fraude de informações podem trazer graves

consequências para a organização, como a perda de mercado, de negócios e, conseqüentemente, perdas financeiras.” Isso eleva a segurança da informação como parte dos negócios empresariais, tendo a mesma relevância quanto as principais aplicações da organização.

As operações realizadas pelo setor financeiro ou comercial, por exemplo, de uma empresa, envolvem diversas transações de dados, tais como, números de cartões de créditos ou contratos, esta inserção de dados deve ser segura, a transmissão protegida e a entrega da informação muito bem armazenada. Estes cuidados devem ser administrados pelo encarregado e coordenador da rede.

Este profissional é diretamente o responsável pela segurança de toda a informação produzida e manipulada e que dependam de meios tecnológicos, influenciando diretamente nos negócios. Para Nakamura e Geus, “é ele o responsável pela definição e implementação da estratégia de segurança das transações eletrônicas e pelo armazenamento de todas as informações” (2007, p.49). Estes encargos e responsabilidades tornam o profissional responsável pela segurança das informações um importante membro nos negócios da organização.

Com a proximidade entre os negócios e a segurança da informação nas organizações, o profissional responsável precisa tratar este tema como prioridade na hora de definir a sua estratégia de segurança. Seguindo as necessidades da empresa, ele tem como trabalho decidir quais tecnologias serão implementadas, e utilizadas, levando em considerações aspectos como desempenho, qualidade e preços, mas acima disso, como elas afetam a segurança das informações, como forma de proteger dados sensíveis da organização bem como aos seus usuários.

Dentre os recursos e ferramentas utilizados dentro de uma organização, destacam-se os navegadores *web*, por sua finalidade como programa e conseqüentemente pela frequência com que é utilizado em função disso. Na seqüência será realizado um estudo referente os navegadores de internet e seus aspectos de segurança. Esta ferramenta é o principal meio de acesso a rede mundial de comunicação, realizando uma espécie de ponte entre o usuário e o conteúdo virtual. A sua utilização já está tão inserida no cotidiano de navegação que sua importância passa despercebida na hora de tomar os devidos cuidados. Em organizações onde os usuários utilizam os navegadores para realizar as operações de seus trabalhos, o responsável pela infraestrutura deve saber identificar e determinar os mais confiáveis a serem utilizados pelos seus usuários.

2.3. FERRAMENTAS DE SEGURANÇA

Novos recursos surgem a cada momento na tecnologia, em contrapartida, métodos para violar estas novidades também acabam por aparecer. É necessário sempre estar atualizado quanto as novidades tecnológicas assim como os perigos que circulam neste ambiente. Existem inúmeras ferramentas e serviços que auxiliam o responsável pela segurança da rede a monitorar, controlar e combater estas ameaças. Fica a critério de cada administrador de redes, selecionar e determinar os mais eficientes para o seu ambiente. Alguns serviços são indispensáveis para qualquer gerenciamento de rede e estão praticamente em qualquer servidor de uma empresa preocupada com a segurança. Devido o tema do trabalho estar direcionado a confiabilidade das informações, serão destacados aqui, ferramentas que possibilitam a verificação deste quesito em específico.

2.3.1. Kali Linux

Ao entrar no tópico referente a ferramentas de segurança, o Kali Linux se destaca entre os seus semelhantes quando a questão são funcionalidades. O Kali Linux é um recurso importante com mais de trezentas ferramentas de segurança e de testes de invasão já instaladas em seu sistema.

Utilizando a distribuição Debian 7.0 como base, o Kali Linux conforme Broad e Bindner “é o *live disk* mais recente de uma distribuição de segurança disponibilizada pela *Offensive Security*” (2014, p. 24). Um sistema operacional utilizado por especialistas em testes de intrusão e auditorias de segurança.

Com um número enorme de ferramentas nativas no próprio sistema operacional, “é possível após instalar esta distribuição Linux, realizar os mais variados testes de segurança como *SQL Inject, Exploits, Sniffers, Scanner, Cracking, Pentests*, entre outros relacionados a comunicação e segurança dos dados” (BROAD; BINDNER, 2014 p. 267).

Esta ferramenta se faz indispensável, tendo em vista que agrega diversas funcionalidades em um único sistema. O Kali Linux estende-se desde um completo sistema operacional para as mais diversas finalidades como servidores e ferramentas de controle do tráfego de informações como firewalls.

2.3.2. Browserscope

O Browserscope é um projeto de código aberto para perfis de navegadores da web com licença Apache 2.0 que foi lançado em setembro de 2009. Esta ferramenta *online* é específica para realização de testes de segurança, executando um total de dezessete testes, analisando o comportamento dos navegadores conforme as ações nos sites em diversos quesitos. Entre alguns de seus testes estão a verificação de aplicativos importantes, como o Java, verificação de quesitos referente a política de segurança, invasões de diversas formas entre outros.

Diferente outras ferramentas com este mesmo objetivo, o Browserscope não necessita da instalação de nenhum plug-in para o seu funcionamento. É possível realizar a comparação dos aplicativos web e verificar a situação referente a cada um. (BROWSCOPE, 2017)

A Tabela 1 apresenta todos os testes realizados pelo Browserscope e ainda, descreve a funcionalidade de cada um. Assim fica compreensível a sua leitura e identificação de cada um juntamente com sua especificação.

Tabela 1 - Descrição dos testes realizados pelo Browserscope

postMessage	Verifica se o navegador suporta a API para mensagens cruzadas do HTML5 para permitir uma comunicação segura entre as origens
JSON.parse	Verifica a existência nativa desta API, este recurso é mais seguro do que outros utilizados como eval
toStaticHTML	Verifica se o navegador suporta esta API que auxilia a intervenção de entradas não confiáveis
httpOnly Cookies	Verifica se o navegador suporta o atributo de cookie httpOnly, uma maneira de conter os ataques de script entre os sites
X-Frame-Options	Verifica se o navegador suporta esta API, que evita ataques de clique, restringindo a forma como as páginas podem ser enquadradas
X-Content-Type-Options	Verifica se o navegador suporta esta API, evitando que alguém visualize o que se está fazendo
Block Reflected XSS	Verifica se o navegador bloqueia a execução do código JavaScript que aparece na URL da solicitação

Block Location Spoofing	Verifica o objeto "location" que pode ser usado pelo JavaScript para determinar em que página ele está executando, é utilizado pelo Flash Player, Google AJAX API e muitos outros programas JavaScripts, os navegadores web devem bloquear os rootkits JavaScripts que tentam substituir este objeto de localização
Block JSON hijacking	Verifica se o navegador bloqueia o sequestro de documentos codificados no formato JSON
Block XSS in CSS	Os scripts para folhas de estilo podem ser usados em um ataque para evitar os filtros XSS no lado do servidor, o Block XSS in CSS realiza esta verificação para garantir que o script injetado em um site por meio da folha de estilo não seja executado
Sandbox attribute	Verifica se o navegador suporta o atributo Sandbox, que permite um conjunto de restrições extras em qualquer conteúdo hospedado pelo iframe
Origin Header	Verifica se o navegador suporta este cabeçalho, que é uma mitigação para ataques de falsificação de solicitações entre sites
Strict Transport Security	Verificado se o navegador é compatível com esta função, pois esta permite que os sites se declarem acessíveis apenas por meio de conexões seguras
Block cross-origin CSS attacks	Verificado se os navegadores bloqueiam ataques CSS de origem cruzada para determinar corretamente o tipo de conteúdo ao carregar recursos deste tipo
Cross Origin Resource Sharing	Verifica se o navegador suporta as APIs que fazem solicitações de origem cruzadas
Block visited link sniffing	O histórico de navegação de um usuário pode ser rastreado testando os links visitados verificando classes CSS, o Block visited link sniffing testa se os navegadores restringem o acesso à pseudo classe visitada
Content Security Policy	Verifica se o navegador é compatível com esta função, o que reduz as superfícies de ataques XSS para sites que desejam optar por estas funcionalidades

Fonte – SITE BROWERSCOPE, (2017)

2.3.3. Sniffers de Rede

Um Sniffer de rede é uma espécie de analisador de pacotes, protocolos ou rede. Segundo Costa “é um programa que opera em modo promíscuo, ou seja, captura e analisa os pacotes que chegam à interface de entrada” (2008, p. 24). Uma ferramenta de muita importância para um gerenciador de redes, devido às inúmeras variações de análise e seleção de dados que um Sniffer pode proporcionar.

Os serviços que estas ferramentas possibilitam exigem muita atenção e cuidados ao serem executados por seus usuários. Devido as suas aplicabilidades e seus métodos operantes, muitas vezes estas ferramentas são utilizadas de forma errônea. Alguns usuários utilizam as funcionalidades dos Sniffers para monitorar dados pessoais de outros usuários da rede, para que se possível roubar estas informações. Se uma rede estiver desprotegida, sem os devidos cuidados na segurança de rede, um Sniffer pode facilmente capturar informações como nomes e senhas de acesso.

Contudo utilizados da maneira correta, um Sniffer traz grandes benefícios aos seus usuários. As funções desta ferramenta auxiliam no acompanhamento de todas as informações que necessitem sair de uma rede interna, para a rede pública. Os dados recolhidos são armazenados pelo programa, e dependendo de qual sniffer o usuário escolher utilizar, suas funcionalidades podem aumentar, como diminuir. Em muitos destes programas, é possível ainda obter informações detalhadas de toda a comunicação realizada, como endereçamento IP, detalhes da origem e do destino, assim como dos tipos de pacotes que estão trafegando. Estas informações fazem toda a diferença no momento de se proteger de algum intruso na rede buscando informações privadas. Existem muitas destas ferramentas no mercado, ficando a cargo do responsável pela infraestrutura qual será escolhida para monitorar todo o tráfego que ocorre em sua rede.

3. NAVEGADORES DE INTERNET

Para realizar uma viagem em alto mar, é praticamente impossível executar esta tarefa sem um veículo apropriado, como um barco ou navio. Este meio de transporte permite aos tripulantes entrar em alto mar e ainda conduzirá de forma rápida e segurança a vários destinos. O oceano é imenso, é possível locomover-se para diversos lugares com diferentes direções. Utilizando esta descrição de navegação marítima, a internet adaptou uma analogia para descrever o seu funcionamento. Assim como um barco se movimenta pelos oceanos, transportando sua tripulação para um determinado destino, os navegadores de internet (*browsers* em inglês) têm por função permitir ao usuário acessar a web e navegar pelo mar de informações dentro dela.

Conforme Comer (2006, p. 322), “um navegador web consiste em um aplicativo que um usuário invoca para acessar e exibir uma página web”. Apesar de seu conceito ser curto e objetivo, a sua importância em prática torna-se muito maior. Este conceito de software foi desenvolvido por Tim Berners-Lee para que um usuário normal através de um computador conseguisse acessar conteúdos web na internet. Por mais que os conceitos de internet e sua primeira aplicação tivessem iniciados à praticamente duas décadas antes, somente em 1995 é que a maioria das pessoas teve a oportunidade de conhecer a web e seus navegadores, (CASTELLS, 2003). Após esse ano a popularização desses conteúdos web aumentou continuamente até os dias atuais e seguem ainda nesse processo, tornando assim os navegadores webs ferramentas essenciais e indispensáveis ao utilizar a internet.

Assim como qualquer outra ferramenta ou serviço, a concorrência entre artefatos com o mesmo propósito se faz presente na categoria dos navegadores. Todos possuem a mesma função: permitir ao usuário acessar e navegar na *web*, porém cada um possui suas próprias características e alguns serviços específicos. Alguns são mais rápidos, outros mais seguros e atualmente todos seguem na disputa pela participação no mercado.

Uma particularidade de cada navegador é a utilização de *plug-ins*. Segundo McClure, Scambray e Kurtz (2014, p. 544), “os plug-ins de navegadores permitem ver e modificar os dados enviados para o servidor remoto em tempo real, enquanto

se navega no site”. Ao ser instalado nos navegadores os *plug-ins* permitem oferecerem aos usuários recursos diferentes do padrão dos navegadores. Alguns navegadores de internet já possuem plug-ins instalados em sua raiz, desta forma no momento em que o usuário instala um navegador, o mesmo já vem com algumas funcionalidades a mais.

Outra característica dos navegadores de internet é a possibilidade de adicionar extensões ao navegador. As extensões permitem incrementar novas funcionalidades ao navegador, permitindo o usuário personalizar sua ferramenta de busca conforme achar melhor. Diferentemente dos plug-ins, as extensões são programas desenvolvidos especialmente para determinados navegadores para criar ou modificar alguma funcionalidade. A existência ou não destes programas não interfere na visualização de páginas web, porém um plugin é necessário muitas vezes para escutar uma musica, por exemplo. (MOZILLA, 2017).

São estas particularidades que cada navegador possui que os diferem de seus concorrentes. O serviço principal é o mesmo, porém alguns quesitos referentes a funcionalidades e principalmente a segurança sempre são levados em consideração pelos seus usuários no momento da escolha de sua ferramenta. Estas singularidades que cada um possui é o que movimenta a disputa pelo mercado entre os navegadores web.

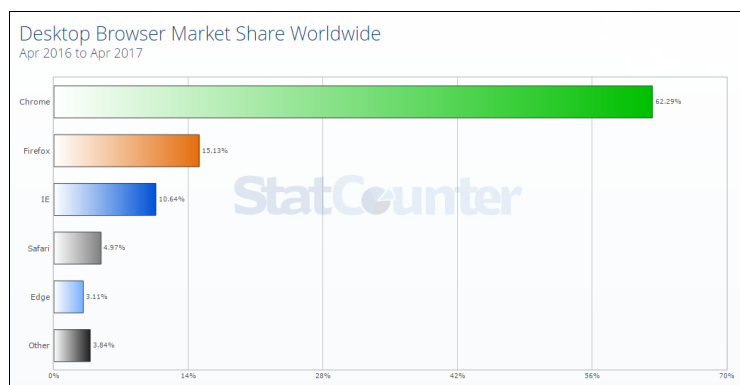
3.1. O MERCADO DOS NAVEGADORES DE INTERNET

A tecnologia da informação sempre está em constante renovação, não é preciso muito tempo para que ferramentas e tecnologias necessitem de atualizações ou se tornem obsoletas. Desde a sua criação muitos navegadores foram desenvolvidos, utilizados e descontinuados com o tempo. Atualmente determinados navegadores dominam o mercado, enquanto outros não obtêm tanta procura. Existem serviços de análises com o objetivo de qualificar os navegadores web mais utilizados por meio de métricas para contabilizar a frequência de uso.

O StatCounter é um serviço de análise da web, que fornece estatísticas independentes e imparciais sobre as tendências de uso da internet, ou seja, realiza os cálculos com base em mais de 15 bilhões de paginas vistas por mês, por pessoas de todo o mundo por meio dos 2,5 milhões de sites membros do grupo.

(STATCOUNTER, 2017). A Figura 1, nos mostra uma análise realizada no período de Abril de 2016 à Abril de 2017, com o objetivo de elencar o Market Share referente aos navegadores para desktops do mundo inteiro.

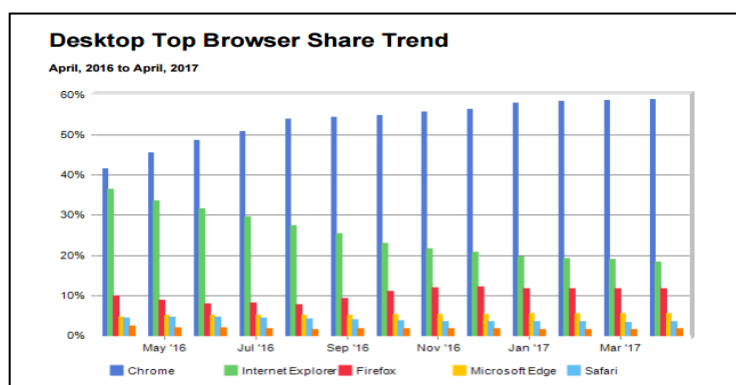
Figura 1 - Market Share dos navegadores para desktops do mundo



Fonte: SITE STATCOUNTER, (2017)

Com o objetivo de obter mais credibilidade na escolha dos navegadores *web* mais utilizados, foi procurado uma segunda referência para este apontamento. O site Netmarketshare.com também é conhecido por apresentar estatísticas de participação dos navegadores, sistemas operacionais e outras tecnologias ascendentes. Desenvolvido pela empresa NetApplications, os seus dados são coletados a partir das visitas únicas diárias em sites rastreados (NETMARKETSHARE, 2017). Abaixo segue a Figura 2, informando os navegadores mais utilizados no mundo, no mesmo período da pesquisa anterior.

Figura 2 - Market Share dos navegadores para desktops do mundo



Fonte – SITE NETMARKETSHARE, (2017)

Existem divergências entre as duas fontes de pesquisas devido às métricas utilizadas por cada empresa para coletar e processar estes dados. Apesar de alguns navegadores estarem em colocações diferentes de uma fonte para outra, nas duas pesquisas existe concordância quanto aos mais utilizados no mundo. Como relatado anteriormente, foram utilizadas duas fontes para esta análise, como forma de certificar os navegadores mais utilizados no mundo.

Com estes dados é possível destacar os navegadores *web* mais utilizados. Seguindo os dados do site StatCounter, em uma escala muito superior encontra-se na liderança o navegador da empresa Google, denominado Chrome, apesar de ser um navegador recente, comparado aos demais, a proposta do Google ganhou preferência na grande maioria dos usuários. Com praticamente 50% do mercado de diferença entre as duas primeiras colocações, segue em segundo a ferramenta da Mozilla, o Firefox. A Microsoft é a única empresa que possui dois produtos na lista dos mais utilizados, o Internet Explorer foi um dos primeiros navegadores apresentados ao mundo em 1995, o qual liderou por anos o topo de pesquisas desse gênero, hoje o Internet Explorer decaiu sua preferência e se mantém na terceira colocação. A Microsoft lançou o substituto do Internet Explorer em 2015 (MICROSOFT, 2017) chamado de Edge que atualmente está na quinta posição do ranking, atrás do Safari da Apple, que apesar de permitir a instalação em outros sistemas operacionais, é um navegador projetado para ser utilizados em ambientes próprios da Apple. O StatCounter por padrão mostra em seu gráfico apenas as cinco primeiras posições, reservando a última para os demais navegadores, onde os nomeia como Outros. Contudo, entre esses outros, se encontra um navegador com participações pequenas no mercado, mas ainda assim, significativas para ser levado em consideração. Em sexto lugar do ranking está o Opera, da empresa Opera Software. Diante do exposto, foram selecionados para realização desta análise, os cinco navegadores mais utilizados: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge e Opera.

3.2. CARACTERÍSTICAS DOS NAVEGADORES DE INTERNET

Conforme visto, existe uma grande variedade de navegadores disponíveis para se acessar a internet. Com a pesquisa realizada na seção anterior foi possível

classificar os mais utilizados atualmente. Apesar de todos terem o mesmo propósito cada um deles possuem suas próprias especificações e características. A seguir é apresentado cada navegador web selecionado para a análise e suas principais características.

3.2.1. Mozilla Firefox

Mozilla Firefox é o navegador disponibilizado pela Fundação Mozilla onde qualquer colaborador tem a possibilidade de contribuir no seu código fonte. Sua primeira versão foi lançada em 2004 com o objetivo de fornecer um produto multi-plataforma simples, seguro e extensível. Por ser um navegador multi-plataforma, o Firefox opera em diversos sistemas operacionais, inclusive alguns não oficializados pela Fundação Mozilla, devido ao fato de possuir seu código-fonte em aberto. Em sistemas Operacionais Linux é encontrado o Firefox já instalado em seu ambiente por padrão. Também é possível encontrar versões portáteis do navegador Firefox, totalmente programado para ser utilizado a partir de pen drives (MOZILLA, 2017).

3.2.2. Internet Explorer

O navegador da Microsoft foi lançado no ano de 1995, por isso esteve por muito tempo no topo da lista dos navegadores mais utilizados. Um dos grandes motivos por sua popularização se deve ao fato do navegador já estar instalado nos ambientes do sistema operacional da Microsoft, o Windows. O Internet Explorer atualmente se encontra na versão 11 e já foi oficializado pela empresa que será a última atualização disponibilizada pela empresa para este navegador, tendo em vista que a Microsoft já lançou o seu substituto, o Microsoft Edge. As versões anteriores do Internet Explorer não recebem mais atualizações da Microsoft porém a versão 11 permanece em algumas versões do Windows 10, principalmente para fins empresariais (MICROSOFT, 2017).

3.2.3. Microsoft Edge

O Microsoft Edge surgiu em 2015 como sucessor do Internet Explorer. Exclusivo para a plataforma Windows mais especificamente para a versão 10 no qual o navegador já vem instalado por padrão. Uma exclusividade do Edge é a inclusão do “Cortana”, assistente de voz pessoal da Microsoft que o usuário pode interagir durante suas buscas (MICROSOFT, 2017).

3.2.4. Opera

Desenvolvido pela empresa Opera Software e lançado publicamente em 1996 o Opera é um navegador multiplataforma, com capacidade de ser instalados nas plataformas Windows, Linux e Mac OS. Entre as principais características do Opera destacam-se o bloqueio de anúncios publicitário e ainda uma VPN gratuita como padrão, estes recursos dispensam a instalação de plug-ins ou extensões ainda que possível. Outra característica interessante é a diminuição do consumo de energia, onde o Opera exige menos processamento quando o mesmo detecta que o computador está fora da tomada. A segurança do navegador possui segurança contra phishing e malware, também verifica sites na web (OPERA, 2017).

3.2.5. Google Chrome

O navegador desenvolvido pela empresa Google e que atualmente domina o mercado de usuários é denominado Google Chrome. Um software multiplataforma e gratuito lançado publicamente no ano de 2008. Existem várias versões do Chrome, inclusive uma com código aberto, denominada Chromium. Este navegador ainda possui uma versão *portable*, que não necessita de instalação na máquina e pode ser executada diretamente de um Pen Drive, por exemplo. (GOOGLE, 2017).

3.3. TRABALHOS CORRELATOS

Esta pesquisa tem como tema a segurança da informação e os conceitos a sua volta, mantendo o foco na confiabilidade dos navegadores de internet. Com o

objetivo de situar essa temática foi realizado uma pesquisa bibliográfica de outros trabalhos relacionados ao tema proposto, os quais serão apresentados a seguir.

A escolha pessoal de uma ferramenta como o navegador de internet difere de um indivíduo para outro. Cada um possui seus critérios particulares que são levados em consideração no momento de determinar a ferramenta a ser utilizada. Em ambientes empresariais, estas escolhas partem dos responsáveis por manter as informações em segurança, divergindo muitas vezes das preferências dos usuários.

Segundo Coelho, (2013), as motivações do uso dos navegadores de internet pelos usuários variam conforme a utilização, tais como, estudos, trabalho, acesso a notícias entre outros. O que leva aos usuários utilizarem navegadores de internet diferentes entre seu uso pessoal e no ambiente de trabalho.

Em sua pesquisa, Coelho (2013) realiza uma análise nos fatores sociais de influência na escolha dos navegadores de internet pelos usuários, nos quais 79,9% destes escolhem sua ferramenta através da reputação/popularidade do navegador.

Outro fator de escolha do navegador importante que a autora utiliza é o tecnológico, onde 93,5% do total de amostras correspondem a velocidade de carregamento das páginas, seguidos da facilidade de navegação (89,2%) e em terceiro a segurança (83,8%) (COELHO, 2013).

A autora em sua pesquisa destinou algumas perguntas voltadas ao grau de confiabilidade dos usuários nos navegadores de internet. Com o maior grau de confiança destacou-se o Google Chrome com 79,9% do total da amostra, seguido pelo Firefox com 69,8% (COELHO, 2013).

Confiar na privacidade que os navegadores de internet oferecem aos usuários é uma questão que deveria exigir mais cuidados. Existem vários métodos na internet que prometem segurança e serviços oferecendo sigilo, (TOLEDO; FEDEL, 2014) trazem em sua pesquisa uma análise sobre a navegação privativa dos navegadores. Por meio de testes e pesquisas os autores têm como objetivo analisar a eficácia deste serviço oferecido por cada navegador.

Conforme Lobato apud Toledo e Fedel, (2014, p. 40) “ao visitar a internet, seja efetuando compras, realizando pesquisas ou mesmo por lazer, o usuário deixa rastros das informações procuradas pela WEB”. Esta afirmação deixa clara a ideia de que nossas informações, preferências e escolhas ficam acessíveis dentro da internet. É possível montar um perfil com muitas informações inseridas pelo usuário. Dependendo do ponto de vista este processo pode ser benéfico ao usuário, pois

quanto mais informações pessoais forem recolhidas, mais sua navegação será adequada para seus propósitos, tornando fácil diversas tarefas como compras e informando novidades do seu interesse. Há porém o outro lado, onde o usuário não possui o conhecimento sobre tais coletas de informações, não sendo estas, claras, objetivas e algumas vezes sem o seu consentimento. Segundo Ishitani apud Toledo e Fedel (2014), este tipo de coleta de informações pode ser considerado como invasão de privacidade, pois o usuário não tem conhecimento de que esta sendo rastreado muito menos consentiu permissão para executar estes serviços.

De acordo com Toledo e Fedel, (2014), a navegação anônima, tema principal do artigo, é um método útil para manter algumas informações privadas e ainda evitar o rastreamento das páginas visitadas. Porém como os próprios autores concluíram, este procedimento é eficaz até certo ponto, pois o endereço IP do usuário continua exposto mesmo em modo anônimo.

A privacidade da informação é o tema principal da pesquisa realizada por Toledo e Fedel (2014), onde não só abordam o conceito de navegação anônima como também trazem assuntos pertinentes quanto a confiabilidade da internet. Conforme os mesmos autores, existem empresas especializadas na vigilância online, os autores citam como exemplo a empresa de tecnologia Google e um de seus serviços mais conhecidos, o provedor de E-mails chamado Gmail. Este serviço já declarou publicamente invadir a privacidade de seus usuários não se importando com a confidencialidade dos e-mails de seus clientes, como consta no próprio termo de compromisso da empresa, da seguinte maneira:

Nossos sistemas automatizados analisam o seu conteúdo (incluindo e-mails) para fornecer recursos de produtos relevantes para você, como resultados de pesquisa customizada, propagandas personalizadas e detecção de *spam* e *malware*. Essa análise ocorre à medida que o conteúdo é enviado e recebido, e quando ele é armazenado. (GOOGLE, 2017)

Em suas considerações finais os autores ainda expõem informações importantes e polêmicas sobre a confidencialidade dos dados. Trazendo novamente a invasão e roubo de informações pessoais como ponto chave para concluir o trabalho. Conforme Toledo e Fedel (2014, p. 50) “diversas corporações faturam bilhões com venda de informações de seus usuários, seja para empresas ou para espionagem governamental”. Tendo em vista os relatos mencionados, é possível

utilizar os mesmos como fonte de pesquisa e ainda como meio de impulsionar este projeto que pretende analisar a confiabilidade dos navegadores.

4. METODOLOGIA

A seguir serão descritos os métodos, equipamentos e ferramentas utilizados para a realização da análise, como a implementação do servidor e cliente e suas configurações necessárias para o processo de testes.

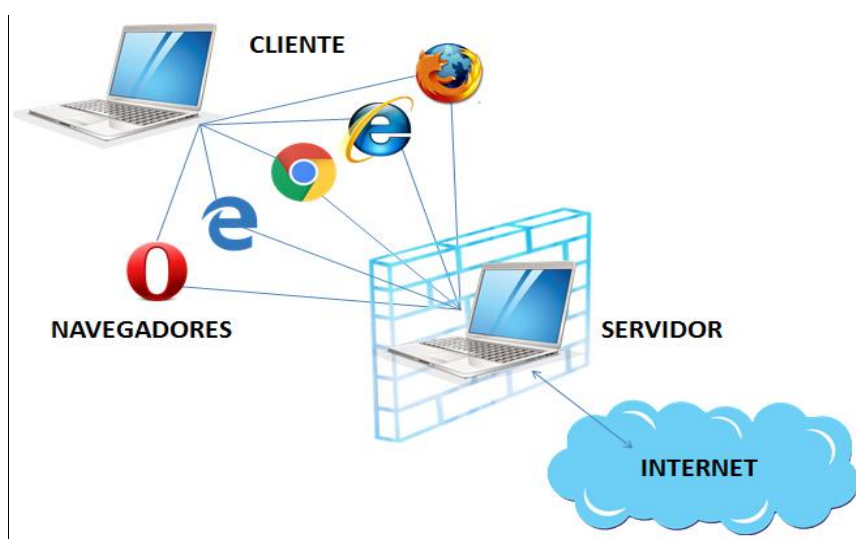
4.1. MÉTODOS E ARQUITETURA

Este estudo foi desenvolvido, a partir de uma pesquisa bibliográfica referente aos navegadores web, com foco na segurança da informação. Conforme definido no objetivo geral do projeto, para analisar a confiabilidade dos navegadores quanto à segurança da informação, é necessário implementar e observar algumas ferramentas e serviços como forma de alcançar resultados significativos. Com base nas informações coletadas no tópico anterior, é possível definir os navegadores *web* mais utilizados pelos usuários.

Com isso os testes e análises foram realizados nos cinco navegadores mais qualificados: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge e Opera. O Safari, navegador da Apple, não foi avaliado nesta análise, pois o mesmo não se encontra disponível oficialmente para Windows, é possível instalá-lo neste ambiente, porém como este navegador é projetado especialmente para rodar em um ecossistema próprio, como é o sistema da Apple, em outros sistemas operacionais pode apresentar comportamentos adversos para o que foi projetado.

Assim, a estrutura elaborada para implementação dos testes de navegadores deste trabalho possui dois notebooks comunicando-se um com o outro por meio de serviços Cliente/Servidor, sendo que o Servidor disponibiliza acesso a internet para o cliente, que por sua vez tem os cinco navegadores de internet, anteriormente mencionados, instalados, acessando a internet e permitindo a realização dos testes. Todo este ambiente de rede que foi desenvolvido e ainda os processos de conexões podem ser visualizados conforme mostra a Figura 3.

Figura 3 - Estrutura de implementação



Fonte: Elaborado pelo autor (2017)

4.2. EQUIPAMENTOS E SISTEMAS

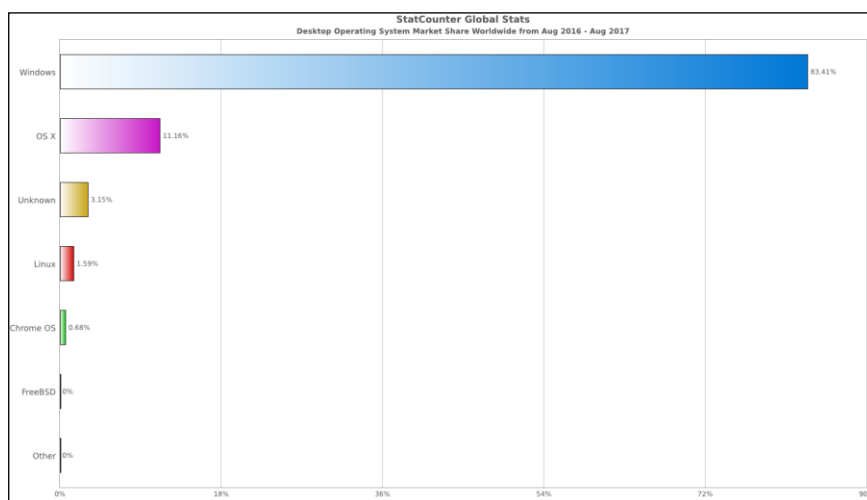
A análise se iniciou a partir da utilização de dois notebooks para a realização dos testes. Uma máquina atendeu a função de Servidor de rede, disponibilizando o acesso a internet para a segunda máquina, Cliente, desta maneira, através do servidor foi possível monitorar o fluxo de dados entre os navegadores e a internet.

A máquina utilizada como Servidor, é um notebook da marca Acer, modelo E1-531-2608, possui um processador Intel Celeron 1000M de 1,8 GHz ainda conta com uma memória RAM de 4 GB e armazenamento interno de 500 GB com o sistema operacional Kali Linux versão 2017.2 instalado.

A segunda máquina ficou definida como Cliente de rede, tendo acesso à internet a partir das configurações definidas no Servidor. Esta máquina foi adquirida especificamente para este propósito, ou seja, é um notebook formatado especificamente para a realização desta análise, sem alterações no sistema operacional para que isto não interferisse nos resultados parciais dos testes.

Por se tratar de uma máquina configurada recentemente, todos os seus programas inclusos são autênticos, inclusive o sistema operacional que para este teste foi utilizado a versão mais recente da Microsoft, o Windows 10. Este sistema foi escolhido pelo fato de ser o sistema operacional mais utilizado segundo dados do StatCounter, conforme mostra a Figura 4 abaixo.

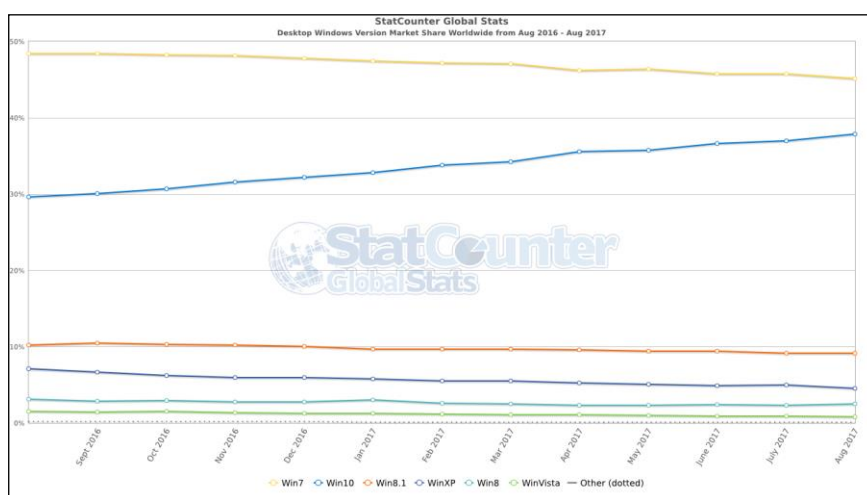
Figura 4 – Desktop Operating System Market Share



Fonte: SITE STATCOUNTER, (2017)

Conforme mencionado anteriormente, a versão do Sistema operacional utilizada para os testes será o Windows 10. Esta é a ultima versão lançada pela Microsoft, por isso a mais atualizada para realizar os testes. A Figura 5 nos mostra que o Windows 7 ainda é predominante no mercado, porém esta sendo descontinuado aos poucos, perdendo espaço e usuários para sua mais recente atualização que em contrapartida cresce gradativamente em utilização nas empresas e por usuários.

Figura 5 – Desktop Windows Version Market Share



Fonte: SITE STATCOUNTER, (2017)

Com base nestes dados, foi possível determinar as escolhas tanto do sistema operacional quanto da sua versão a serem utilizadas nesta pesquisa. Também se buscou utilizar softwares atualizados e hardware com um bom desempenho para obter resultados claros e sem interferências. Sendo assim, a máquina² que foi utilizada como Cliente, é um notebook da marca DELL pertencente ao modelo Inspiron i15-5566-A10P com uma capacidade de processamento Intel Core i3 de 2,0 GHz, conta com uma memória RAM de 4 GB e armazenamento interno de 1 TB.

4.3. FERRAMENTAS E SERVIÇOS

Com os equipamentos a disposição, deu-se início a fase de instalações e configurações das ferramentas e serviços utilizados nos testes. Na máquina, destinada ao Servidor, foi realizada a instalação e configuração necessária para que o Cliente se conecte à internet através do mesmo, não permitindo nenhuma comunicação do cliente com a internet fora destas especificações.

O servidor foi completamente instalado e configurado manualmente. Após seu download no site autorizado da comunidade Kali Linux, iniciou-se a instalação na máquina atribuída para este serviço. Com o Sistema operacional em funcionamento foi realizada a configuração das interfaces de rede nas duas máquinas para obter e disponibilizar o acesso a internet via cabo *crossover*.

Alguns serviços necessitam ser configurados para que este método de comunicação se torne possível. A estrutura básica de interfaces de rede e configuração da faixa de endereçamento IP disponibilizada para o acesso do cliente são elementos importantes e indispensáveis para uma comunicação estável e segura.

Com a arquitetura montada, as máquinas se comunicando e as ferramentas instaladas, a próxima etapa é a preparação de todo o âmbito que será realizado os testes. Estas configurações são os ajustes necessários para dar início aos testes programados.

4.3.1. BrowserScope

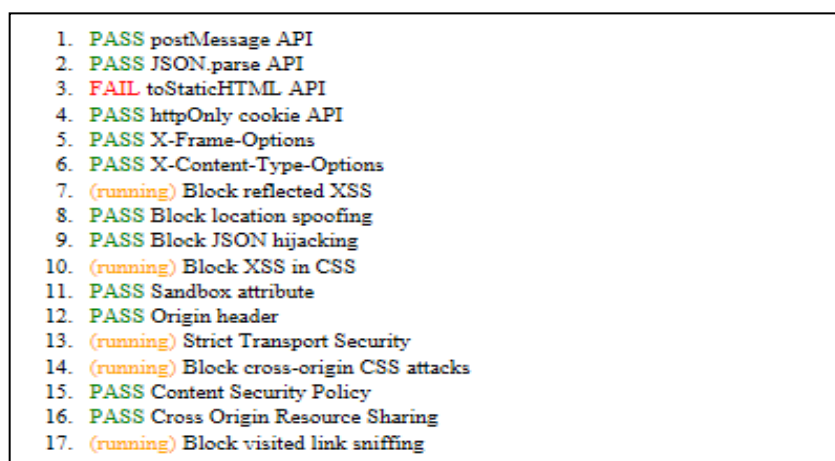
Ao concluir a verificação inicial das ferramentas pré-instaladas nos navegadores de forma manual, ou seja, buscando nas configurações de cada sistema os serviços instalados que compõem cada navegador, no seguinte teste será utilizada uma ferramenta própria para este perfil de verificação.

O recurso Browserscope é necessário para uma análise mais profunda e interna nos navegadores web. Verificando funcionalidades de difícil acesso a usuários manualmente, o Browserscope realiza uma varredura no navegador web para encontrar e analisar funções que contribuem ou prejudicam o sistema.

O sistema de análise do Browserscope é executado diretamente no navegador. Por ele é possível acessar o site da ferramenta onde se encontram diversos meios para executar os testes. Com a página de testes pronta para ser executada, foi realizado um número determinado de dez testes do mesmo gênero para cada navegador selecionado.

O tempo de execução para cada teste varia entre quatro à cinco minutos, desta maneira a execução repetidas vezes em cada navegador diminuem as probabilidades de erros ou seja, os dados obtidos serão mais específico se em caso de alguma das execuções o resultado de um dos testes divergir. Na Figura 6 abaixo é possível visualizar como ocorre o processo de testes em um dos navegadores web, retornando para cada teste *Pass* (Passou) para uma execução bem-sucedida ou *Fail* (Falhou) em caso do navegador falhar em determinado exame.

Figura 6 – Exemplo de teste em andamento utilizando Browserscope



1.	PASS	postMessage API
2.	PASS	JSON.parse API
3.	FAIL	toStaticHTML API
4.	PASS	httpOnly cookie API
5.	PASS	X-Frame-Options
6.	PASS	X-Content-Type-Options
7.	(running)	Block reflected XSS
8.	PASS	Block location spoofing
9.	PASS	Block JSON hijacking
10.	(running)	Block XSS in CSS
11.	PASS	Sandbox attribute
12.	PASS	Origin header
13.	(running)	Strict Transport Security
14.	(running)	Block cross-origin CSS attacks
15.	PASS	Content Security Policy
16.	PASS	Cross Origin Resource Sharing
17.	(running)	Block visited link sniffing

4.3.2. HTML5 Test

O html5test.com é outra ferramenta para realizar testes nos navegadores web com o objetivo de identificar os mais adeptos a tecnologia do HTML5. Diferentemente do Browserscope que é totalmente voltado para a parte de segurança, o HTML5 Test realiza um escaneamento em diversos aspectos dos navegadores. Sua análise percorre serviços como performance, integração, conectividade, multimídias e ainda uma avaliação na segurança dos navegadores. (HTML5 TEST)

Ao se executar os testes, este serviço entrega um resultado total da soma de cada funcionalidade que a ferramenta requisita e que o navegador possui. Cada especificação que o navegador possui conforme as exigidas pelo teste são adicionada como um ponto, somando todos no final podendo chegar a quinhentos e cinquenta e cinco pontos se todos os critérios forem cumpridos. A página inicial contendo o resultado de um teste executado como exemplo é apresentado na Figura 7 abaixo.

Figura 7 – Exemple resultado de teste utilizando HTML5 Test

Security		21/32
Web Cryptography API	Yes	✓
Content Security Policy 1	No	✗
Content Security Policy 2	No	✗
Cross-Origin Resource Sharing	Yes	✓
Subresource Integrity	Yes	✓
Cross-document messaging	Yes	✓
Authentication		
Web Authentication / FIDO 2	No	✗
Credential Management	No	✗
Iframes		
Sandboxed iframe	Yes	✓
iframe with inline contents	Yes	✓

Fonte: SITE HTML5 Test, (2017)

Ainda é possível visualizar a pontuação de cada navegador por grupo de análise, como por exemplo, gráficos e efeitos e em outros dispositivos de acesso. São vinte e seis grupos de análise que também apresentam suas pontuações particulares.

Para este trabalho o único grupo que se faz relevante é o que aborda os testes de segurança e confiabilidade. Este grupo de análise verifica dez funcionalidades que os navegadores devem possuir como APIs, protocolos de segurança e métodos de autenticação. Ao final, se todas as especificações forem atendidas este grupo recebe o total de trinta e dois pontos e informando ao lado de cada uma se o navegador possui (Yes) ou não (No).

4.3.3. Wireshark

O Wireshark é o sniffer de rede escolhido para realizar os testes de tráfego de informações. Conforme visto na sessão 2.3.4 este conceito de ferramenta é indispensável para monitoramentos e abstração de tudo que esta ocorrendo na rede interna.

Conforme Morimoto, o Wireshark “é um sniffer bastante completo que permite capturar o tráfego de rede, fornecendo uma ferramenta poderosa para detectar problemas e entender melhor o funcionamento de cada protocolo”. (MORIMOTO, 2011, p. 446). O Wireshark é capaz de detalhar cada pacote capturado, fornecendo muitas informações referentes ao mesmo. Ao clicar no pacote desejado, é possível visualizar informações pertinentes para um acompanhamento confiável entre origem e destino das informações.

O usuário deste software precisa ter conhecimento dos verdadeiros objetivos desta ferramenta, ou seja, fornecer um controle de tudo que entra e sai da rede possibilitando detectar qualquer tipo de *trojan* ou acesso não autorizado.

4.4. AMBIENTE E METODOLOGIA DE TESTES

Com os sistemas operacionais devidamente instalados nas máquinas e configurados para suas atividades iniciou-se a configuração do ambiente para a realização dos testes, como instalação dos softwares e criação dos elementos necessários na análise.

Na máquina Cliente, com o sistema operacional Windows10, foi instalado a versão mais recente e atualizada dos cinco navegadores selecionados. Muitas vezes é importante ter conhecimento de qual versão de software está sendo utilizado para

ajudar a solucionar um problema ou simplesmente saber se está atualizado. No Internet Explorer a versão do navegador mais recente utilizada nesta análise é a 11.608.15063.0, o Google Chrome encontra-se na versão 61.0.3163.100, o Mozilla Firefox foi instalado com a 55.0.3, Opera com a versão 48.0.2685.35 e o Microsoft Edge 40.15063.0.0.

O download dos navegadores de internet foi efetuado nos sites autorizados das empresas responsáveis pelos seus desenvolvimentos, para evitar cópias ou programas maliciosos. Com o download concluído realizou-se a instalação dos navegadores na máquina Cliente e realizada a primeira análise para verificar a existência de plug-ins ou extensões dispensáveis juntamente neste processo.

Para a realização dos testes de análise de tráfego, foi utilizada uma conta de E-mail pessoal para melhor acompanhar esta troca de informação. Desta maneira é possível além de realizar os testes em navegação normal pelos sites, ainda verificar uma conta de E-mail onde o usuário encontra-se *logado* no sistema.

4.4.1. Ajustes dos Navegadores de Internet

Ao iniciar a etapa de testes, a primeira verificação e configuração nos navegadores foi realizada após a instalação dos mesmos. Para que a análise ocorresse da forma mais justa e correta possível, foi procurado e desativado qualquer plug-in, extensão ou complemento já instalado no navegador, estruturando um ambiente limpo para a realização dos testes, sem perigo de interferência destes programas.

O Internet Explorer é disponibilizado com poucos complementos já instalados. É um navegador que não necessita de instalação, pois já está incluso no sistema operacional do Windows 10 por padrão, com ele, encontra-se instalado os plug-ins do antivírus também disponibilizado e instalado pela Microsoft. Todos os complementos foram desativados para o seguimento dos testes de acordo com as especificações, conforme a Figura 8 a seguir.

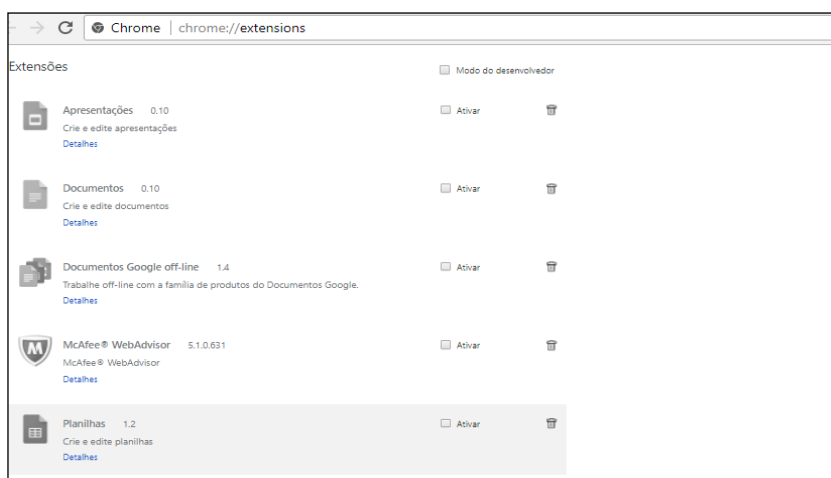
Figura 8 – Complementos Internet Explorer desativados

Gerenciar Complementos					
Exibir e gerenciar complementos do Internet Explorer					
Tipos de Complemento	Nome	Fornecedor	Status	Arquitetura	Tempo...
Barras de Ferramentas e Extensões Provedores de Pesquisa Aceleradores Proteção contra Rastreamento	McAfee, Inc.				
	McAfee WebAdvisor BHO	McAfee, Inc.	Desabilitado	32 bits e 64...	
	Microsoft Corporation				
	Lync Click to Call	Microsoft Corporation	Desabilitado	64 bits	
	Lync Browser Helper	Microsoft Corporation	Desabilitado	64 bits	
	XML DOM Document	Microsoft Corporation	Desabilitado	32 bits e 64...	
	Não disponível				
	OneNote Linked Notes	Não disponível	Desabilitado	32 bits e 64...	
	McAfee WebAdvisor	Não disponível	Desabilitado	32 bits e 64...	
	Send to OneNote	Não disponível	Desabilitado	32 bits e 64...	

Fonte: Elaborado pelo autor, (2017)

O Google Chrome teve uma alteração em seu gerenciamento de plug-ins após a versão 57. Esta atualização torna o navegador mais fechado para o usuário pois impede o acesso à alguns plug-ins instalados, dificultando a sua desativação. Um exemplo desses plug-in, instalado diretamente em seu núcleo é chamado de Shockwave Flash, de difícil acesso para a anulação, este plug-in continuou em funcionamento. As demais extensões ativas por padrão no navegador como leitor de PDF, planilhas e ainda a extensões do antivírus foram inativadas conforme a Figura 9 abaixo.

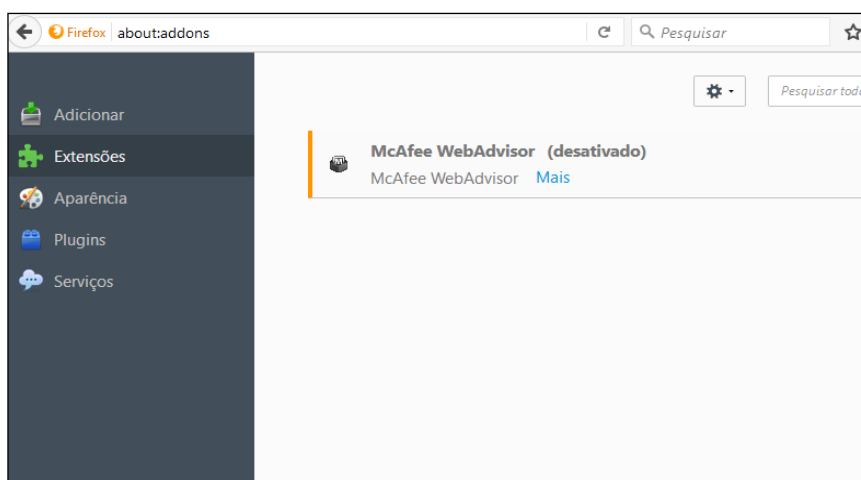
Figura 9 – Extensões Chrome desativadas



Fonte: Elaborado pelo autor, (2017)

No navegador da Mozilla, o Firefox, a manipulação de plug-ins e extensões é um processo acessivelmente simples e descomplicado. No menu de plug-ins apenas dois são encontrados e são utilizados para a codificação e proteção de vídeos. Quanto as extensões apenas a do antivírus foi encontrada no sistema. Tanto os plug-ins quanto a extensão encontrada por padrão já estão ativas no sistema e foram desativadas para a procedência dos testes conforme mostra a Figura 10 abaixo.

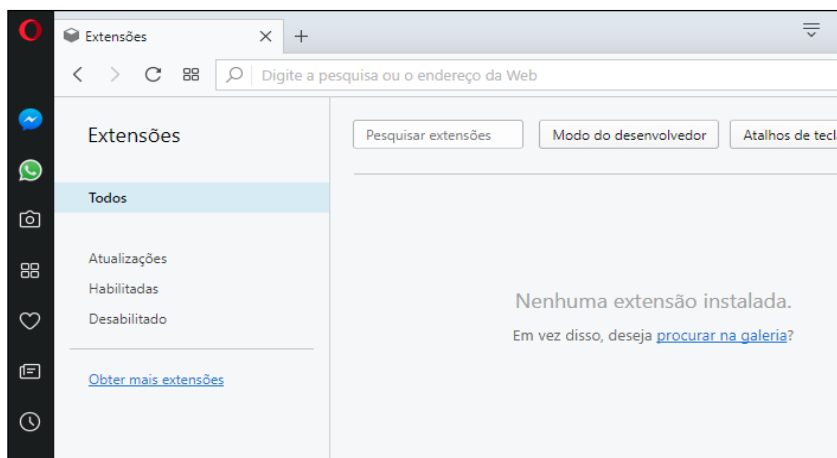
Figura 10 – Extensões Firefox desativadas



Fonte: Elaborado pelo autor, (2017)

Com o navegador Opera não são encontrados plug-ins instalados em seu sistema. Ao entrar na página gerenciadora das extensões também não são encontrados nenhum serviço deste gênero na listagem, porém ao acessar a janela gerenciadora de tarefas do Opera é possível visualizar a extensão Background worker em funcionamento. Esta extensão renderiza as páginas web e possui um processo complicado para ser desinstalada do navegador, não sendo possível executar esta ação na extensão. Na Figura 11 é possível observar a janela de configurações das extensões vazia.

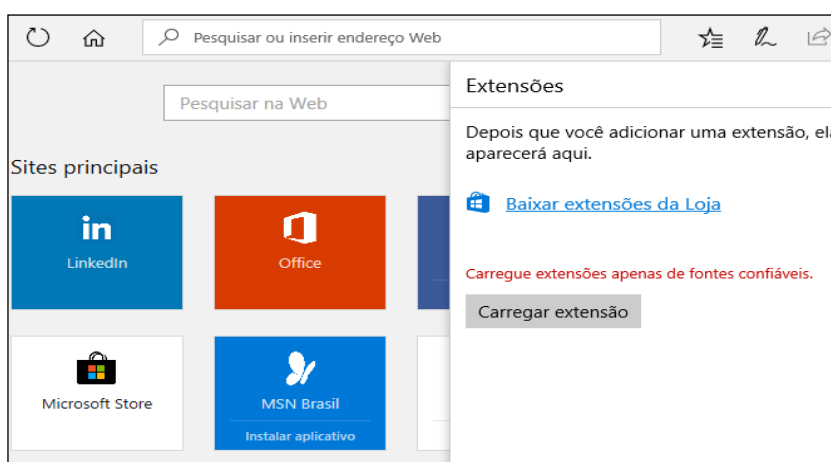
Figura 11 – Extensões Opera desativadas



Fonte: Elaborado pelo autor, (2017)

O mais novo navegador da Microsoft, o Edge não possui extensões instaladas em seu sistema. Seu ambiente de configurações para as ferramentas já instaladas no navegador é de difícil acesso, impossibilitando configurações ou alterações neste ambiente. A janela de configuração do Edge pode ser visualizada na Figura 12 abaixo.

Figura 12 – Extensões Edge desativadas



Fonte: Elaborado pelo autor, (2017)

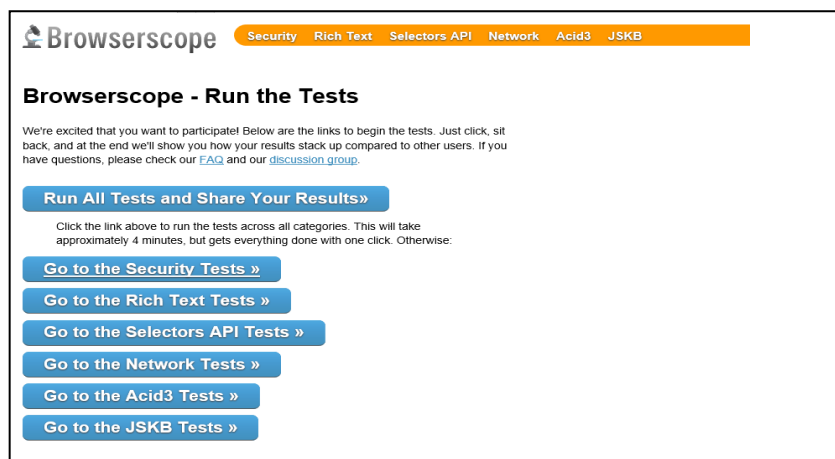
4.5. METODOLOGIA DA REALIZAÇÃO DOS TESTES

Através das pesquisas foi possível definir alguns métodos para que auxiliassem nesta análise. Deste modo, foi possível encontrar ferramentas disponíveis na internet com um alto nível de confiabilidade, muitas delas gratuitas e de fácil acesso, viabilizando mais proteção e acompanhamento das informações por profissionais interessados.

4.5.1. BrowserScope

Com cada teste especificado e uma compreensão correta do Browserscope como descritos na sessão 2.3.3 deste projeto, deu-se início a execução dos testes utilizando esta ferramenta. A Figura 13 abaixo mostra a página para a seleção dos testes do Browserscope, acessada pelo endereço <http://www.browserscope.org/>.

Figura 13 – Seleção de Testes Utilizando Browserscope



Fonte: SITE BROWSERSCOPE, (2017)

4.5.2. HTML5 Test

Esta ferramenta é inicializada automaticamente ao acessar seu endereço *online*. Isto facilita sua utilização e a compreensão das informações que o teste gera. Para cada navegador recém instalado na máquina e com o histórico de navegação

totalmente apagado, foi acessado o endereço de teste e capturado todos os resultados obtidos.

4.5.3. Wireshark

Os testes utilizando esta ferramenta transcorreram entre acessar uma série de páginas web pelo cliente e monitorar o fluxo de pacotes gerados no servidor utilizando o Wireshark. Foram determinados diferentes endereços web para os acessos, com o intuito de testar vários ambientes, contendo requisitos como segurança, *login* e algumas ações de *upload* e *download* para arquivos.

O primeiro passo deste teste foi iniciar o Wireshark no Servidor para capturar o tráfego e logo em seguida abrir o navegador a ser verificado no Cliente para iniciar os testes de acessos aos endereços web determinados. Cada teste foi executado utilizando apenas um navegador por vez durante cinco repetições, ou seja, os outros navegadores ficavam fechados enquanto o selecionado realizava sua sequência de acessos. Este seguimento de acessos se fazia da mesma forma para todos os outros navegadores utilizados na análise, bem como o tempo de duração de cada série de teste. Ao encerrar uma sequência de acessos, parava-se a execução do Wireshark, salvando o *script* gerado com todas as informações referentes ao tráfego e acessos do Cliente. O principal critério a ser avalizado neste teste é a quantidade de pacotes que o navegador de internet gera enquanto esta conectado a internet.

4.5.3.1. Teste de Minuto Sem Navegação

No primeiro teste de captura de pacotes, foi utilizado uma metodologia simples, onde se iniciava o navegador web e sem realizar nenhuma ação o mesmo ficava estático durante o período de um minuto. Após este período encerrava-se o navegador juntamente com a captura de tráfego. Com isso é possível observar a quantidade de pacotes gerados em cada navegador sem realizar nenhuma ação.

4.5.3.2. Teste de Minuto Com Navegação

A segunda sequência de testes utilizando o Wireshark transcorre da mesma maneira que a anterior porém durante o período de um minuto é realizado o acesso a uma página web com autenticação. Ao iniciar o Wireshark, o navegador é executado e redirecionado para o endereço da página web selecionado. Os três sites testados separadamente foram <http://inf.passofundo.ifsul.edu.br/>, <https://www.americanas.com.br/> e https://moodle.passofundo.ifsul.edu.br. Estes sites foram selecionados por conter diferentes métodos de segurança, sendo que um utiliza o protocolo HTTP, o outro HTTPS e por fim um HTTPS com certificação. Os três sites possuem formulário de autenticação de usuário, ao acessar a página era efetuado o *login*. Após este processo, não se realizava nenhuma ação, aguardando ao término do minuto para então parar o Wireshark.

4.5.3.3. Teste Completo de Navegação

Para a última sequência de testes foi destinado um número maior de acessos consecutivos a páginas web. Ao total são seis destinos que o navegador após inicializado tem que acessar ininterruptamente.

A primeira página acessada é o serviço de webmail, Gmail, disponibilizado no endereço: <https://mail.google.com>. Uma conta com *login* de acesso se faz importante para a análise referente a confidencialidade da informação, uma vez que ao entrar em um sistema propriamente fechado, suas informações devem prevalecer em segurança. Este *site* também possui HTTPS, ou seja, a comunicação é criptografada, aumentando assim a segurança dos dados.

Para acessar o serviço de webmail foi utilizado uma conta já existente, este endereço de E-Mail também será utilizado em outras páginas de testes, isto porque esta conta já possui tempo de utilização, contendo vínculos com outros sistemas de *login*. A Figura 14 a seguir mostra a primeira página de teste acessada com os campos de validação preenchidos.

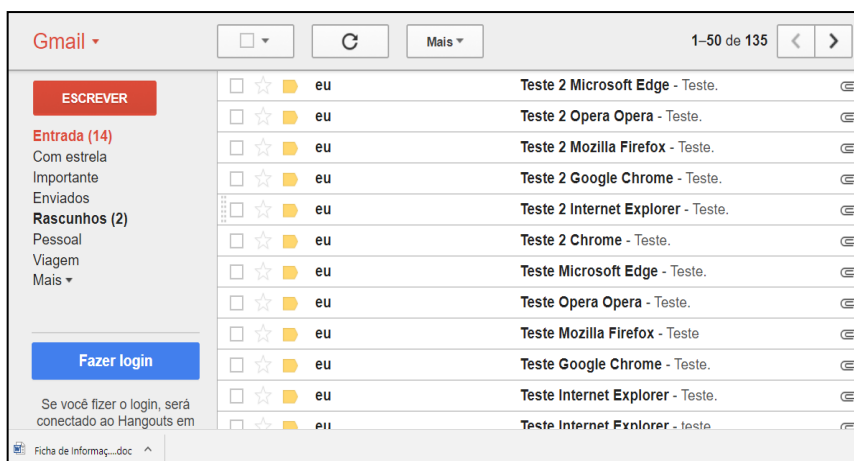
Figura 14 – Página de teste Gmail



Fonte: Elaborado pelo autor, (2017)

Ainda *logado* neste serviço de *webmail*, foi realizado mais algumas ações como parte do teste. Uma destas operações foi o envio de um E-Mail contendo um anexo, com o objetivo de acompanhar o tráfego gerado por este serviço e ainda, como outra operação, foi realizado o download de um arquivo com o mesmo propósito. Na Figura 15 é possível acompanhar estas ações sendo realizadas.

Figura 15 – Teste de envio de E-Mail e download de arquivo



Fonte: Elaborado pelo autor, (2017)

Prosseguindo com os testes, o próximo endereço acessado é outro site com proteção HTTPS, denominado Q-Acadêmico, disponível no endereço: <https://qacademico.ifce.edu.br/>. É um serviço de interação acadêmica entre

professores e alunos. Abaixo segue a Figura 16 da página de autenticação do Q-Acadêmico.

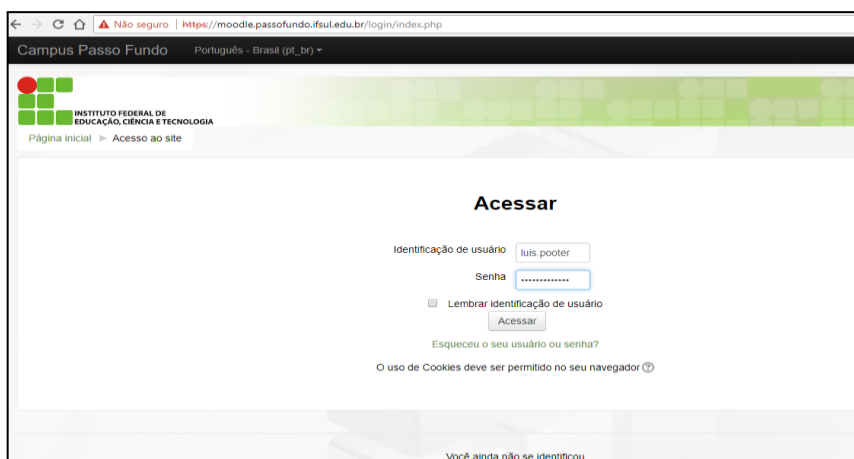
Figura 16 – Página de autenticação do sistema Q-Acadêmico



Fonte: Elaborado pelo autor, (2017)

Em seguida, um site com diferentes métodos de segurança, o Moodle, disponibilizado no endereço: <https://moodle.passofundo.ifsul.edu.br>. É um software livre de apoio a aprendizagem, que gerencia por meio da instituição de ensino suas tarefas entre outras funções. Como possui um protocolo de segurança desigual ao anterior, este serviço foi escolhido para a realização do teste como forma de diversificar os acessos nas páginas web. Este procedimento pode ser visualizado na Figura 17 abaixo, contendo os dados de entrada ao sistema.

Figura 17 – Página de autenticação do sistema Moodle



Fonte: Elaborado pelo autor, (2017)

Para o terceiro serviço a ser acessado, foi selecionado uma página de compras *online*. A loja virtual Americanas esta entre as primeiras colocadas de uma seleção das maiores empresas e-commerce brasileira (MELIUZ, 2017). Por esta razão este site foi selecionado para realizar outro teste de acesso e está disponível no endereço: <https://www.americanas.com.br/>. Por conter o protocolo HTTPS e também um sistema de cadastro, foi utilizado a mesma conta de E-Mail para realizar login no sistema e verificar suas ações com o tráfego de informações em um sistema de comércio *online*. A Figura 18 a seguir, mostra a página de identificação do cliente no site.

Figura 18 – Página de autenticação do E-Commerce Americanas

Seguro | <https://cliente.americanas.com.br/simple-login/?next=https%3A%2F%2Fwww.americanas.com.br%2F%23>

americanas.com

identificação

e-mail:

senha na americanas.com: [esqueci minha senha](#)

continuar

ou

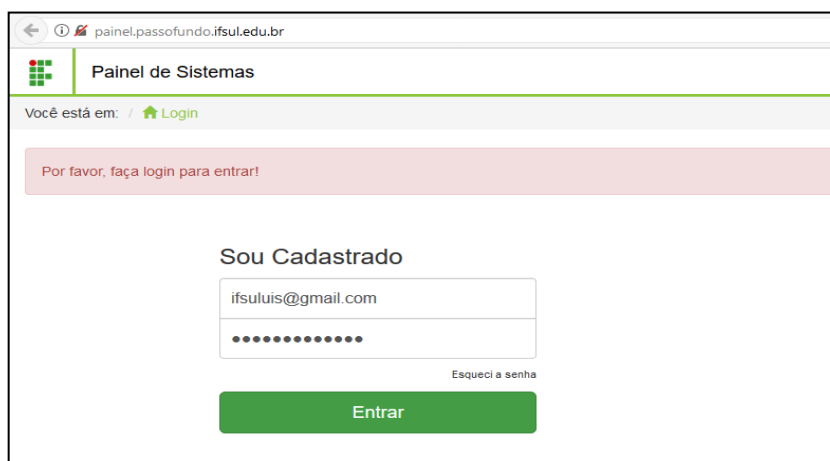
Continuar com o Facebook

Não tem cadastro? [cadastre-se](#)

Fonte: Elaborado pelo autor, (2017)

Ainda, o seguinte acesso web foi o painel de sistemas do curso de informática IFSUL, disponibilizado no endereço: <http://painel.passofundo.ifsul.edu.br/>. Este site é um gerenciador dos sistemas ofertados pela instituição de ensino como cadastros, inscrições e acompanhamentos por parte dos usuários. Como aluno, foi utilizado a mesma conta de E-Mail para o acesso ao sistema e continuidade no teste. Este site foi selecionado por possuir seu protocolo de comunicação como HTTP, o que diferencia dos acessos anteriores, trazendo mais diversidade na análise. A Figura 19 a seguir, mostra a página mencionada.

Figura 19 – Página de autenticação do E-Commerce Americanas



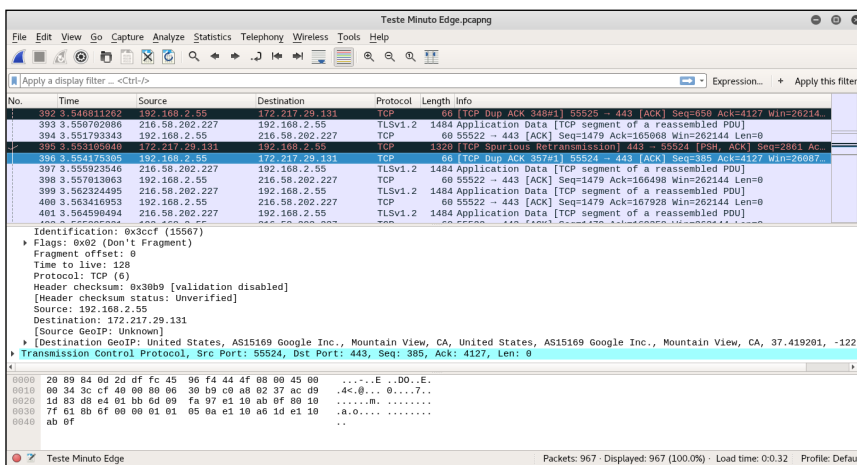
The screenshot shows a web browser window with the address bar displaying 'painel.passofundo.ifsul.edu.br'. The page title is 'Painel de Sistemas'. Below the title, there is a navigation bar with 'Você está em: / Login'. A red banner contains the message 'Por favor, faça login para entrar!'. The main content area is titled 'Sou Cadastrado' and contains a login form with two input fields: the first contains the email 'ifsuluis@gmail.com' and the second contains masked characters. A link 'Esqueci a senha' is located below the password field. A green button labeled 'Entrar' is positioned at the bottom of the form.

Fonte: Elaborado pelo autor, (2017)

Por fim, o último *site* acessado e utilizado nesta sequência de testes é a plataforma de distribuição de vídeos digitais YouTube, disponível no endereço: <https://www.youtube.com/>. Este *site* é dedicado a vídeos, onde usuários podem publicar vídeos em formato digital. Esta página foi escolhida para realizar o teste pela sua diversidade juntamente as outras apresentadas anteriormente, tendo em vista que sua finalidade é totalmente diferente das demais, trazendo assim endereços web utilizados com frequência por usuários em geral.

Com isso, após todas as páginas de testes serem acessadas e seus devidos requisitos executados, foi encerrado o navegador web e interrompido o programa Wireshark no servidor. Um relatório foi gerado para cada teste realizado, contendo todas as capturas do tráfego dos protocolos produzidos durante o teste. Os relatórios foram devidamente salvos, para em seguida serem analisados e comparados com os demais testes dos outros navegadores. A seguir com a Figura 20 é possível visualizar uma parte de todos os protocolos capturados pelo Wireshark.

Figura 20 – Exemplo de captura de pacotes efetuado pelo Wireshark



Fonte: Elaborado pelo autor, (2017)

5. RESULTADOS OBTIDOS

Com os testes estabelecidos devidamente executados, os resultados foram analisados tendo como ângulo os objetivos traçados pela pesquisa. Este capítulo é disposto de subseções que apresentam os resultados obtidos em todos os testes realizados.

5.1. RESULTADOS DOS TESTES UTILIZANDO BROWSERSCOPE

Conforme apresentado na Tabela 2, a grande maioria dos requisitos solicitados pelo Browserscope foram cumpridos por parte dos navegadores. Apenas três testes retornaram resultados negativos para seus respectivos navegadores e unicamente o teste referente a compatibilidade do navegador com HSTS (HTTP Strict Transport Security) novo padrão de segurança SSL que força a utilização do HTTPS demonstrou instabilidade, não completando o teste. Em nenhum navegador este quesito foi concluído, mesmo utilizando outra máquina para teste, o que comprova uma falha no Browserscope diante desta verificação.

Tabela 2 - Resultado do teste utilizando o Browserscope

TESTE	CHROME	FIREFOX	IE	OPERA	EDGE
postMessage API	Pass	Pass	Pass	Pass	Pass
JSON.parse API	Pass	Pass	Pass	Pass	Pass
toStaticHTML API	Fail	Fail	Pass	Fail	Fail
httpOnly cookie API	Pass	Pass	Pass	Pass	Pass
X-Frame Options	Pass	Pass	Pass	Pass	Pass
X-Content-Type-Options	Pass	Pass	Pass	Pass	Pass
Block Reflected XSS	Pass	Pass	Pass	Pass	Pass
Block Location Spoofing	Pass	Pass	Pass	Pass	Pass
Block JSON hojacking	Pass	Pass	Pass	Pass	Pass
Block XSS in CSS	Pass	Pass	Pass	Pass	Pass
Sandbox Attribute	Pass	Pass	Pass	Pass	Pass
Origin header	Pass	Fail	Fail	Pass	Pass
Strict Transport Security	Running	Running	Running	Running	Running
Block cross-origin CSS attac	Pass	Pass	Pass	Pass	Pass
Content Security Policy	Pass	Pass	Fail	Pass	Pass
Cross Origin Resource Shari	Pass	Pass	Pass	Pass	Pass
Block visited link sniffing	Pass	Pass	Pass	Pass	Pass

O teste que verifica se o navegador suporta a API toStaticHTML foi o que obteve menos aprovações. Nesta avaliação, a API para desinfecção de entradas não confiáveis foi encontrada somente no Internet Explorer. Contudo este mesmo navegador foi o único que falhou no teste de Política de Segurança do Conteúdo, que verifica a compatibilidade do navegador com Content Security Policy, que reduz as superfícies de ataques de injeção de conteúdos, tais como XSS.

Por fim, outro teste que obteve falha por parte dos navegadores foi o Origin Header, sendo que o Internet Explorer e o Firefox não passaram neste quesito. Este recurso ameniza ataques do tipo *cross-site request forgery* que explora a confiança que um *website* tem no navegador do usuário.

5.2. Resultados dos testes utilizando HTML5 Test

A Tabela 3 abaixo mostra os resultados obtidos com a ferramenta HTML5 Test. Com o resultado posicionado desta maneira é possível visualizar cada teste realizado pelo recurso bem como as pontuações individuais de cada requisito e ainda a soma total que cada navegador conquistou.

Tabela 3 - Resultado do teste utilizando o HTML5 Test

TESTE	PONTOS	CHROME	FIREFOX	IE	OPERA	EDGE
Web Cryptography API	5	YES	YES	YES	YES	YES
Content Security Policy 1	3	NO	NO	NO	YES	YES
Content Security Policy 2	2	YES	NO	NO	YES	YES
Cross-Origin Resource Sharing	4	YES	YES	YES	YES	YES
Subresource Integrity	2	YES	YES	NO	YES	NO
Cross-document messaging	2	YES	YES	YES	YES	YES
Web Authentication / FIDO 2	3	NO	NO	NO	NO	PARTIAL
Credential Management	3	YES	NO	NO	YES	YES
Sandboxed iframe	4	YES	YES	YES	YES	YES
iframe with inline contents	4	YES	YES	NO	YES	NO
TOTAL	32	26	21	15	29	23

Fonte: Elaborado pelo autor, (2017)

A vantagem de realizar testes semelhantes em ferramentas distintas é a constatação dos resultados se relacionarem. Alguns testes realizados no HTML5 Test se assimilam aos executados com o Browserscope, e o resultado também é compatível entre ambos em sua grande maioria. Apenas o teste referente a Política de Segurança do Conteúdo obteve divergência entre as verificações, sendo que o Firefox também apresentou falha neste quesito pelo HTML5 Test.

No teste de Autenticação na Web utilizando o protocolo FIDO 2 para comunicação entre um autenticador externo e outro cliente, praticamente todos os navegadores reprovaram, apenas o Microsoft Edge obteve parcialmente êxito neste quesito, não alcançando completamente os requisitos exigidos. O Opera foi o navegador que mais somou pontos nesta análise, falhando apenas na verificação descrita a pouco. Seguido pelo Chrome, Edge, Firefox e com a menor pontuação o Internet Explorer, reprovando em mais da metade dos testes executados.

5.3. Resultados dos testes utilizando wireshark

Utilizando a ferramenta Wireshark é possível realizar os mais variados tipos de testes referentes ao tráfego de pacotes. Para esta análise será limitado à verificação e comparação da quantidade de pacotes gerados em cada navegador. Com os mesmos acessos e tempo de realizações iguais para cada teste, o número de pacotes trafegados na rede possuem uma quantidade semelhante, não divergindo em grandes proporções.

5.3.1. Resultado: Teste de Minuto Sem Navegação

O primeiro teste utilizando a ferramenta Wireshark é exibido na Tabela 4 a seguir, com ele é possível verificar a diferença dos números de pacotes gerados de um navegador para outro durante a sua inicialização no tempo de um minuto. Com os mesmos acessos, em tempo de execução igual para todos, o número de pacotes transferidos não deve distanciar demasiadamente um dos outros.

Tabela 4 - Quantidade de pacotes capturados durante um minuto sem navegação

NAVEGADORES	Nº PACOTES (por minuto)
Internet Explorer	606
Mozilla Firefox	418
Google Chrome	554
Microsoft Edge	967
Opera	520

Fonte: Elaborado pelo autor, (2017)

O número de pacotes transferidos durante a utilização de cada navegador em teste pode ser observado na coluna da direita desta tabela. Com apenas um teste, utilizando uma metodologia simples, sem navegação ou autenticação em sistemas fechados, onde apenas é inicializado o navegador, já é possível observar números elevados na comparação destes programas.

Estes dados são apresentados em uma tabela para melhor e mais rápida compreensão, contudo, as imagens contendo as informações detalhadas referentes a este teste podem ser encontradas no Apêndice A deste trabalho.

5.3.2. Resultado: Teste de Minuto Com Navegação

Com a execução do segundo teste fica visível a comparação entre cada navegador diante do acesso as páginas selecionadas. Ainda que todas as informações estejam apresentadas em uma única tabela, cada teste foi executado separadamente.

A Tabela 5 a seguir demonstra o número de pacotes capturados em cada navegador web, durante o tempo de um minuto ao acessar cada página descrita na seção 4.3.4.2 e ainda realizar *login* em cada uma delas.

Tabela 5 - Quantidade de pacotes capturados durante um minuto com navegação

NAVEGADORES	MOODLE	INF	AMERICANAS
Internet Explorer	1900	5600	15781
Mozilla Firefox	1349	4997	11786
Google Chrome	2026	4489	13590
Microsoft Edge	2483	6072	18820
Opera	1896	4590	13498

Fonte: Elaborado pelo autor, (2017)

Como apresentado no teste anterior, onde foi utilizada uma abordagem simples, neste outro, aplicando a mesma metodologia de tempo e processos de execução, porém agora, acessando conteúdos e realizando autenticações, como resultado é apresentado às mesmas variações na quantidade de pacotes transferidos durante o teste.

Estes dados são apresentados em uma tabela para melhor e mais rápida compreensão, contudo, as imagens contendo as informações detalhadas referentes a este teste podem ser encontradas no Apêndice B deste trabalho.

5.3.3. Resultado: Teste Completo de Navegação

A Tabela 6 apresenta os resultados da última bateria de testes utilizando o Wireshark. É possível visualizar cada navegador e o número total de pacotes gerados durante os sucessivos acessos as páginas. Este teste foi realizado três vezes com cada navegador, sempre com os mesmos critérios e metodologias definidas, definidas anteriormente na seção 4.5.3.3. O tempo de execução para cada teste também eram observados para não divergirem. Esta sequência repetitiva do mesmo teste aumenta o número de dados a serem coletados, facilitando sua análise e comparação.

Tabela 6 - Quantidade de pacotes capturados durante um minuto com navegação

NAVEGADORES	1° Sequência	2° Sequência	3° Sequência
Internet Explorer	49237	52644	50612
Mozilla Firefox	45179	49973	47933
Google Chrome	40332	44681	48312
Microsoft Edge	49770	54751	52759
Opera	42684	41907	45699

Fonte: Elaborado pelo autor, (2017)

Por ser o último teste realizado, a metodologia empregada ainda se assemelha aos executados nas seções 5.3.1 e 5.3.2, porém com um número mais amplo de acessos web e autenticações consecutivas. Como produto disto, o que foi capturado e analisado neste, apenas comprova e finaliza todos os testes executados anteriormente. Sendo que, o resultado em números reais, de todos os testes realizados nesta seção, confirmam divergências entre os navegadores quanto a transferências de protocolos e informações na rede e ainda, evidenciam alguns navegadores que tendem a esta prática.

Estes dados são apresentados em uma tabela para melhor e mais rápida compreensão, contudo, as imagens contendo as informações detalhadas referentes a este teste podem ser encontradas no Apêndice C deste trabalho.

De acordo com o exposto nos resultados obtidos a partir dos testes realizados, é possível se chegar a algumas conclusões sobre a questão da confiabilidade dos navegadores de internet mais utilizados no mercado, conforme segue.

6. CONCLUSÃO

Com o tema exposto na presente pesquisa, torna-se inevitável não chegar a um consenso de que a segurança da informação é um dos temas mais amplos e importantes relacionados a tecnologia computacional. Todo o referencial teórico apresentado descreve anos de pesquisas e descobertas, deixando claro que este tema sempre estará passível de mais estudos, tendo em vista que a tecnologia se renova constantemente.

Tendo em vista os objetivos traçados para a realização desta análise, é possível afirmar que todas as etapas parciais definidas para alcançar o objetivo geral desta pesquisa, foram cumpridas com êxito. Os estudos dos principais conceitos e tecnologias foram essenciais para compreensão e aprofundamento sobre o tema da pesquisa.

Cada navegador selecionado para a análise, com ajuda de dados comprobatórios, pôde ser devidamente reconhecido, através de suas características apresentadas, e analisado. Os critérios e métodos para a realização da avaliação dos navegadores foram definidos como proposto, trazendo para conhecimento geral, ferramentas úteis, necessárias ao realizar uma avaliação destacando a segurança, como foi a utilização do Browserscope, ou uma ferramenta mais abrangente em testes, como o HTML5 Test. Ainda, o Wireshark se demonstrou uma excelente ferramenta para captura do tráfego de pacotes na rede. Desta forma, foi possível analisar todos os dados obtidos nos testes realizados, como proposto.

A partir do primeiro teste realizado com a ferramenta Browserscope, foi possível identificar uma falha na verificação de um dos requisitos exigidos, onde todos os navegadores não concluíram esta etapa. Os demais testes transcorreram normalmente com resultados equivalentes em muitos casos. O quesito que mais apontou falha nos navegadores foi o teste de verificação da API toStaticHTML, neste apenas o Internet Explorer passou. Contudo este navegador juntamente com o Firefox, foram os únicos a reprovar em dois testes. A verificação do cabeçalho Origin header, reprovou estes dois navegadores nesta avaliação. Outro teste que obteve uma única falha foi a verificação da compatibilidade do navegador com a política de segurança de conteúdo, onde somente o Internet Explorer reprovou.

O HTML5 Test se demonstrou uma ferramenta mais categórica em suas verificações. Mesmo com menor número de testes, comparado ao Browserscope, este teste detectou mais falhas nos navegadores dentre os exigidos para qualificação. Seu sistema de pontuação para cada verificação auxilia na compreensão da relevância de cada teste ao atribuir uma nota máxima ou parcial.

Neste teste, todos os navegadores apresentaram irregularidade em pelo menos um teste. O Opera conquistou o menor número de falhas, reprovando em apenas um teste, neste em questão todos os outros navegadores reprovaram. Em seguida estão o Chrome e o Edge, com problemas em duas verificações. No Firefox o índice aumentou para quatro reprovações. E por fim, o Internet Explorer com o maior número de testes reprovados. Ao total são seis falhas, somando apenas quinze pontos, quatorze a menos se comparado ao Opera, navegador que totalizou vinte e nove pontos dos trinta e dois possíveis.

Por fim, o teste mais representativo, utilizando o Wireshark, apresentou resultados instigantes para a análise. A utilização básica desta ferramenta é fácil com rápida aprendizagem, porém é necessário um conhecimento experiente para executar funções mais específicas do programa.

O Wireshark como visto, captura todos os pacotes que trafegam na rede interna, quando são enviados e recebidos, todos podem ser observados. Este programa ainda totaliza o número exato de pacotes que passam pelo servidor. Este dado é a premissa para esta análise, pois sua expressão como número torna visível e imparcial uma comparação entre os navegadores testados.

Em todos os testes de captura e análise de tráfego, os navegadores Edge e Internet Explorer respectivamente, se sobressaíram na quantidade de pacotes que trafegaram na rede quando os mesmos foram utilizados.

A quantidade de tráfego dos dados no Microsoft Edge ficou, em todos os testes realizados, muito acima dos demais navegadores. Ainda, é seguido pelo seu antecedente, o Internet Explorer, que também se coloca em segundo lugar, quanto ao número de pacotes percorridos, em todos os testes. Opera, Chrome e Firefox possuem uma quantidade de fluxo semelhantes, não distanciando assim, um dos outros, e alterando suas posições no *ranking* a cada teste realizado.

Não é possível assegurar a confidencialidade das informações apenas com os números totais obtidos. O número de pacotes que trafegam na rede é imenso, em uma conexão sem navegar em outras páginas web, no tempo de um minuto, como

visto no teste realizado na seção 4.3.1, a média de pacotes recebidos e enviados é de seiscentos e treze. Já em um teste mais amplo, com navegação e autenticação em outras páginas web, também no mesmo tempo de um minuto, como descrito na seção 4.3.2, este número se amplia consideravelmente para os próximos de dois mil pacotes transferidos.

Com estas quantidades exorbitantes de pacotes gerados a cada ação no navegador, conseqüentemente aumenta a demanda em analisar os dados contidos em cada um. Como visto nas seções 1.3.2 e 3.3.3, referentes aos sniffers de rede e a ferramenta utilizada, Wireshark, podemos identificar nos pacotes capturados, entre outros informes, para qual destino as mensagens foram enviadas. Esta informação contribui para a verificação da rota correta dos dados inseridos nos navegadores, preservando a confidencialidade do navegador ao manipular informações privadas, caso o destino venha a ser desconhecido.

Contudo, para está análise, tornou-se impossível a verificação de cada pacote em questão, devido a sua grande quantidade versus o período para análise. Sendo que, vários testes foram executados e para cada um, repetidas realizações.

Com isso, é definido que a quantidade total de pacotes capturados, por si só, não condiz necessariamente com a falta ou excesso de segurança na informação. Contudo, é instigante que alguns navegadores demandem de um número consideravelmente maior de protocolos do que outros, para processarem as mesmas informações e requisitos, no mesmo espaço de tempo.

Em conjunto, o resultado dos testes realizados em todas as ferramentas, levando em consideração os números elevados de tráfego, como um possível ponto negativo para a confidencialidade, tendo em vista que, outros navegadores realizam os mesmos processos com menoridade na transferência das informações, é possível destacar navegadores menos propensos a confidencialidade.

Sendo assim, somos levados e considerar, sempre apoiados aos resultados obtidos, que existem navegadores com inclinação a problemas no tratamento da segurança das informações. Os navegadores *open source* demonstraram ênfase no quesito da confidencialidade. Uma das vantagens de sistemas com código aberto, sendo que aumenta consideravelmente o número de colaboradores dispostos a corrigir uma falha ou melhorar alguma particularidade.

Os navegadores Opera, Firefox e Chrome, obtiveram resultados semelhantes nos testes. Entre estes, nenhum apresentou resultados consistentes, que

demonstrem problemas na segurança e confidencialidade das informações. É importante ressaltar que a versão utilizada do Chrome possui seu código fonte fechado, mesmo assim, este navegador obteve resultados positivos nos testes realizados, contrariando as incitações de falta de segurança e sigilo.

Todavia os navegadores Edge e Internet Explorer apresentaram resultados intrigantes nos testes realizados. O mais recente navegador do mercado, Edge obteve resultados positivos nos testes utilizando o Browserscope e HTML5 Test, se igualando ao demais navegadores. Porém ao analisar o tráfego na rede utilizando o Edge, a quantidade de pacotes que são transmitidos com sua utilização é comprovadamente maior do que qualquer outro navegador, conforme todos os testes realizados na seção 4.3 desta análise.

Contudo, é o Internet Explorer que diante dos testes, evidenciou mais problemas de acordo com a segurança. Desde o teste utilizando o Browserscope, no qual apresentou falhas incomuns aos demais navegadores. Passando ainda pelo teste HTML5 Test, no qual foi o navegador que mais apontou falhas na sua verificação, somando a menor pontuação entre todos. Por fim, mesmo o Edge possuindo o maior número de pacotes transferidos, o Internet Explorer, não fica muito distante neste teste, mantendo-se em segundo lugar em todas as verificações executadas, conforme mostra a seção 4.3 desta análise.

Diante das etapas realizadas, conclui-se que os aspectos de segurança dos navegadores diferem quando comparados em um âmbito homogêneo. É possível sim distinguir estes programas quanto a sua segurança e principalmente confidencialidade garantida por cada um. Com isso, fica evidente que o problema exposto para esta análise, possui soluções cabíveis a serem empregadas para que em ambientes corporativos, os responsáveis pela segurança optem por ferramentas que ofereçam o máximo de segurança e sigilo para suas informações.

Ao realizar uma análise desta envergadura, é necessário tempo e dedicação para o estudo e construção de um trabalho que contemple todas as etapas necessárias. Inicialmente o maior desafio, se fazia em construir uma rede interna com um cliente e servidor que comunicassem entre eles. Contudo este processo foi elaborado e concluído rapidamente sem grandes dificuldades. O grande desafio foi encontrar ferramentas específicas para realização de testes com ênfase na confidencialidade dos navegadores de internet. Existem poucas ferramentas com este objetivo, sendo que nenhuma concede um resultado concreto para este quesito.

É necessário agrupar os resultados de outros testes realizados e analisá-los com devido cuidado.

Com as contribuições que esta análise proporcionou, ficam resultados significativos a serem considerados em sua finalização. Como mencionado na introdução deste trabalho, a tecnologia da informação está em constante renovação, com isso as limitações aqui encontradas, podem servir como impulso para trabalhos futuros. A verificação de cada pacote que trafega na rede é uma análise importante a ser abordada de maneira mais aprofundada futuramente, pois se trata de um processo que demanda tempo para verificação devido ao grande fluxo de protocolos na rede, porém com a sua realização poderá ser comprovado uma possível emissão de dados para destinos não autorizados.

Cabe ressaltar, que por se tratar de uma área ampla, conforme o tema abordado na presente pesquisa, a segurança de redes sempre apresentará novas possibilidades a serem estudadas e desenvolvidas. Especificamente em ambientes corporativos, a obtenção e manutenção de um ambiente seguro deve ser constantemente perseguida e periodicamente revisada. Esse processo passa fundamentalmente pela compreensão e análise dos mais variados elementos envolvidos nesse meio, como foi o caso dos navegadores de internet aqui pesquisados.

REFERÊNCIAS

BROAD, James; BINDNER, Andrew. **Hacking com Kali Linux: Técnicas práticas para testes de invasão**. Novatec, 2014.

BROWERSCOPE. **Browserscope FAQ**. Disponível em: <<http://www.browserscope.org/faq>>. Acesso em: Agosto/2017

CASTELLS, Manuel. **A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade**. Zahar, 2003.

COELHO, Milena de Lima Cavalcanti. **Impacto dos perfis tecnológicos na escolha e no comportamento de uso de navegadores de internet**. 60 f. Monografia (bacharelado) – Administração, Universidade de Brasília, 2013.

COMER, Douglas E. **Interligação de Redes com TCP/IP**. Elsevier, 2006.

COSTA, Daniel Gouveia. **Java em Rede**. Brasport, 2008.

FONTES, Edison. **Segurança da Informação: O usuário faz a Diferença**. Saraiva, 2006.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. Bookman, 2013.

GOOGLE. **Google Terms of Service**. Disponível em: <<https://www.google.com.br/chrome/browser/privacy/utos-text.html>>. Acesso em: Maio/2017.

HTML5 TEST. **How well does your browser support html5?**. Disponível em: <<https://html5test.com/>>. Acesso em: Novembro/2017.

INTERNET EXPLORER. **Suporte da Microsoft**. Disponível em: <<https://support.microsoft.com/pt-br/help/969393/information-about-internet-explorer>>. Acesso em: Maio/2017

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. **Hackers Expostos – 7ed: Segredos e Soluções para a Segurança de Redes**. Bookman, 2014.

MELIUZ. **As 50 Melhores Lojas Online do Brasil**. Disponível em: <<https://www.meliuz.com.br/blog/50-melhores-lojas-brasil/>>. Acesso em: Setembro/2017.

MICROSOFT EDGE. **Suporte da Microsoft**. Disponível em: <<https://privacy.microsoft.com/pt-br/windows-10-microsoft-edge-and-privacy>>. Acesso em Abril/2017.

MORAES, Alexandre Fernandes de. **Segurança em Redes – Fundamentos**. Érica, 2010.

MORIMOTO, Carlos Eduardo. **Redes: Guia Prático**. Sul Editores, 2011.

MOZDEV. **Plugins: para que servem e como instalar?** Disponível em: <<http://br.mozdev.org/firefox/plugin>>. Acesso em: Agosto/2017.

MOZILLA. **Suporte Mozilla**. Disponível em: <<https://support.mozilla.org/pt-BR/products/firefox>>. Acesso em Maio/2017

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de Redes em ambientes corporativos**. Novatec, 2007.

NETMARKETSHARE. **Desktop Top Browser Share Trend, April 2016 to April 2017**. Disponível em: <<https://www.netmarketshare.com/>>. Acesso em: Abril/2017.

OPERA. **Opera Software**. Disponível em: <<http://help.opera.com/Windows/10.20/pt/history.html>>. Acesso em: Maio/2017.

STATCOUNTER GLOBAL STATS. **Desktop Browser Market Share Worldwide, April 2016 to April 2017**. Disponível em: <<http://gs.statcounter.com/browser-market-share/desktop/worldwide/#monthly-201604-201704-bar>>. Acesso em: Abril/2017.

TOLEDO, André Yuri; FEDEL, Gabriel de Souza. **Privacidade na WEB: uma análise sobre a navegação privativa dos navegadores**. Tecnologia em Segurança da Informação, Faculdade de Tecnologia de Americana, 2014.

APÊNDICE A - Resultado Teste de Minuto Sem Navegação

Figura 21 – Teste de conexão sem navegação em um minuto com Internet Explorer

No.	Time	Source	Destination	Protocol	Length	Info
194	9.287747187	192.168.2.55	172.217.29.227	TCP	60	56114 → 443 [ACK] Seq=205 Ack=1431 Win=262144 Len=0
195	9.288233838	172.217.29.227	192.168.2.55	TCP	1484	443 → 56114 [ACK] Seq=1431 Ack=205 Win=44032 Len=1430 [TCP segme...
196	9.288242398	172.217.29.227	192.168.2.55	TLSv1.2	1320	Certificate, Server Key Exchange, Server Hello Done
197	9.288486697	172.217.29.227	192.168.2.55	TLSv1.2	1484	Server Hello
198	9.288691206	172.217.29.227	192.168.2.55	TCP	1484	443 → 56115 [ACK] Seq=1431 Ack=205 Win=44032 Len=1430 [TCP segme...
199	9.289054658	192.168.2.55	172.217.29.227	TCP	60	56114 → 443 [ACK] Seq=205 Ack=4127 Win=262144 Len=0
200	9.292496289	192.168.2.55	172.217.29.227	TCP	60	[TCP Dup ACK 178#1] 56115 → 443 [ACK] Seq=205 Ack=1 Win=262144 L...
201	9.292496182	172.217.29.227	192.168.2.55	TLSv1.2	1320	Certificate, Server Key Exchange, Server Hello Done
202	9.292795121	192.168.2.55	172.217.29.227	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes...
203	9.292811961	192.168.2.55	172.217.29.227	TCP	66	[TCP Dup ACK 178#2] 56115 → 443 [ACK] Seq=205 Ack=1 Win=262144 L...
204	9.293070817	192.168.2.55	172.217.29.227	TLSv1.2	141	Application Data
205	9.293212536	192.168.2.55	172.217.29.227	TLSv1.2	297	Application Data
206	9.294604350	172.217.29.227	192.168.2.55	TCP	66	443 → 56118 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK...
207	9.295659666	192.168.2.55	172.217.29.227	TCP	60	56118 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
208	9.296620938	192.168.2.55	172.217.29.227	TLSv1.2	258	Client Hello
209	9.336179136	172.217.29.227	192.168.2.55	TLSv1.2	125	Application Data
210	9.336192237	172.217.29.227	192.168.2.55	TLSv1.2	100	Application Data
211	9.336608396	192.168.2.55	172.217.29.227	TCP	60	56113 → 443 [ACK] Seq=1277 Ack=68608 Win=261840 Len=0

Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0xed32 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.2.55
 Destination: 172.217.29.227
 [Source GeoIP: Unknown]
 [Destination GeoIP: United States, AS15169 Google Inc., Mountain View, CA, United States, AS15169 Google Inc., Mountain View, CA, 37.419201, -122.5]

Transmission Control Protocol, Src Port: 56115, Dst Port: 443, Seq: 205, Ack: 1, Len: 0

0000 20 89 84 0d 2d df fc 45 96 f4 44 4f 08 00 45 00E..DD..E.
 0010 00 34 7f f5 40 00 80 06 ed 32 c0 a8 02 37 ac d9 .(.@...j....7..

Packets: 606 · Displayed: 606 (100.0%) · Load time: 0:0.25 · Profile: Default

Fonte: Elaborado pelo autor, (2017)

Figura 22 – Teste de conexão sem navegação em um minuto com Firefox

No.	Time	Source	Destination	Protocol	Length	Info
226	6.838275765	192.168.2.55	172.217.29.227	TLSv1.2	248	Application Data
227	6.840176208	8.8.4.4	192.168.2.55	DNS	234	Standard query response 0x07de A www.gstatic.com A 172.217.29.22...
228	6.840188121	8.8.4.4	192.168.2.55	DNS	248	Standard query response 0x0c7e A apis.google.com CNAME plus.l.go...
229	6.841336060	192.168.2.55	192.168.2.50	DNS	75	Standard query 0x8b95 AAAA www.gstatic.com
230	6.846535633	192.168.2.55	172.217.29.227	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes...
231	6.847533055	192.168.2.55	172.217.29.238	TCP	66	56176 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER...
232	6.848285094	192.168.2.55	172.217.29.227	TLSv1.2	248	Application Data
233	6.866680388	172.217.29.227	192.168.2.55	TLSv1.2	338	New Session Ticket, Change Cipher Spec, Encrypted Handshake Mess...
234	6.866693815	172.217.29.227	192.168.2.55	TLSv1.2	123	Application Data
235	6.867055614	192.168.2.55	172.217.29.227	TCP	60	56174 → 443 [ACK] Seq=480 Ack=4480 Win=66048 Len=0
236	6.867458446	192.168.2.55	172.217.29.227	TLSv1.2	85	Encrypted Alert
237	6.867481194	192.168.2.55	172.217.29.227	TCP	60	56174 → 443 [FIN, ACK] Seq=511 Ack=4480 Win=66048 Len=0
238	6.868563785	172.217.29.227	192.168.2.55	TLSv1.2	92	Application Data
239	6.868863242	192.168.2.55	172.217.29.227	TCP	60	56174 → 443 [RST, ACK] Seq=512 Ack=4518 Win=0 Len=0
240	6.873669053	172.217.29.227	192.168.2.55	TLSv1.2	338	New Session Ticket, Change Cipher Spec, Encrypted Handshake Mess...
241	6.873681961	172.217.29.227	192.168.2.55	TLSv1.2	123	Application Data
242	6.873694165	172.217.29.227	192.168.2.55	TLSv1.2	92	Application Data
243	6.874042894	192.168.2.55	172.217.29.227	TCP	60	56175 → 443 [ACK] Seq=480 Ack=4517 Win=66048 Len=0

Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0x6ad5 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.2.55
 Destination: 172.217.29.227
 [Source GeoIP: Unknown]
 [Destination GeoIP: United States, AS15169 Google Inc., Mountain View, CA, United States, AS15169 Google Inc., Mountain View, CA, 37.419201, -122.5]

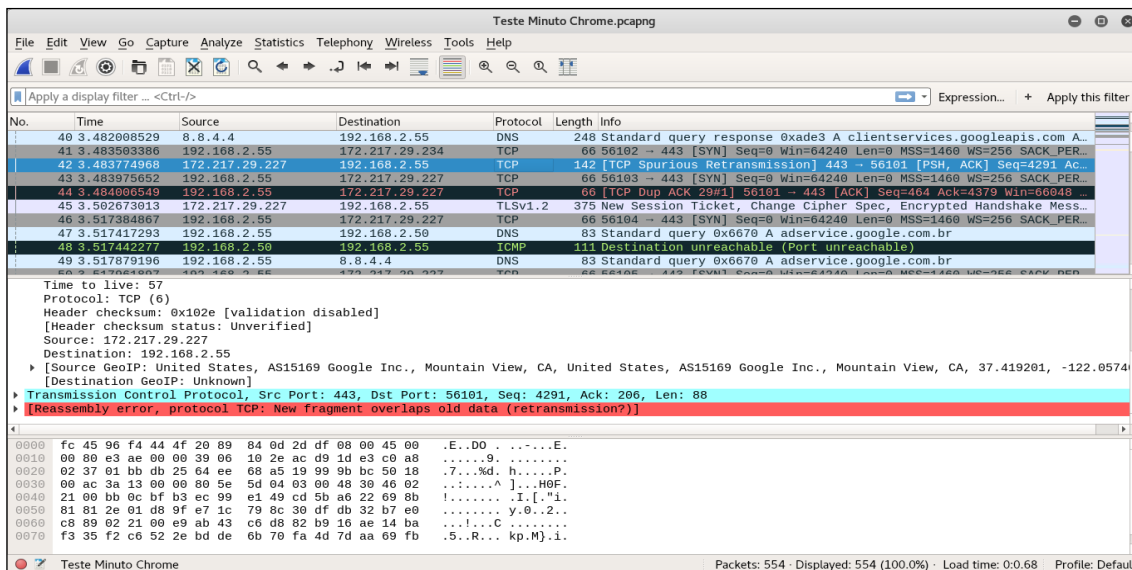
Transmission Control Protocol, Src Port: 56174, Dst Port: 443, Seq: 512, Ack: 4518, Len: 0

0000 20 89 84 0d 2d df fc 45 96 f4 44 4f 08 00 45 00E..DD..E.
 0010 00 28 02 5f 40 00 80 06 6a d5 c0 a8 02 37 ac d9 .(.@...j....7..

Packets: 418 · Displayed: 418 (100.0%) · Load time: 0:0.14 · Profile: Default

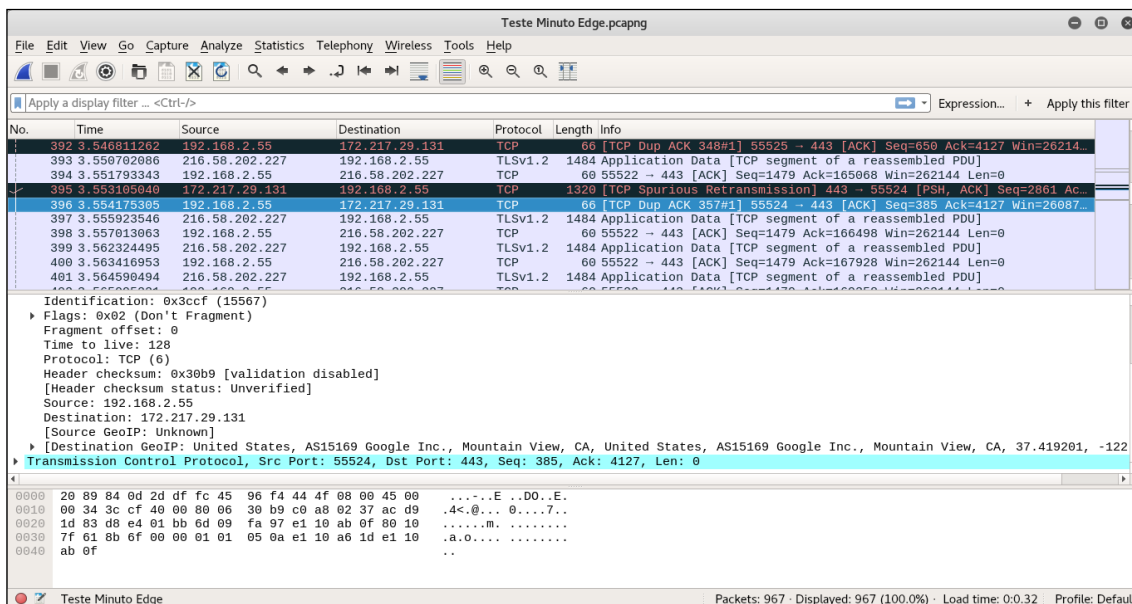
Fonte: Elaborado pelo autor, (2017)

Figura 23 – Teste de conexão sem navegação em um minuto com Chrome



Fonte: Elaborado pelo autor, (2017)

Figura 24 – Teste de conexão sem navegação em um minuto com Edge



Fonte: Elaborado pelo autor, (2017)

Figura 25 – Teste de conexão sem navegação em um minuto com Opera

No.	Time	Source	Destination	Protocol	Length	Info
315	4.611038637	192.168.2.55	107.167.110.216	TCP	60	56090 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
316	4.611061609	192.168.2.55	107.167.110.216	TCP	60	56088 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
317	4.611078727	192.168.2.55	107.167.110.216	TCP	60	56089 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
318	4.611397582	192.168.2.55	107.167.110.216	TLSv1.2	262	Client Hello
319	4.611530995	192.168.2.55	107.167.110.216	TLSv1.2	262	Client Hello
320	4.611646225	192.168.2.55	107.167.110.216	TLSv1.2	262	Client Hello
321	4.637065983	172.217.29.227	192.168.2.55	TCP	54	443 → 56077 [ACK] Seq=70745 Ack=1829 Win=48384 Len=0
322	4.809387510	107.167.110.216	192.168.2.55	TCP	54	443 → 56090 [ACK] Seq=1 Ack=209 Win=30720 Len=0
323	4.809406847	107.167.110.216	192.168.2.55	TCP	54	443 → 56088 [ACK] Seq=1 Ack=209 Win=30720 Len=0
324	4.810331828	107.167.110.216	192.168.2.55	TLSv1.2	1494	Server Hello
325	4.810343294	107.167.110.216	192.168.2.55	TLSv1.2	1494	Certificate [TCP segment of a reassembled PDU]
326	4.810352672	107.167.110.216	192.168.2.55	TLSv1.2	171	Server Key Exchange, Server Hello Done
327	4.810362207	107.167.110.216	192.168.2.55	TCP	54	443 → 56089 [ACK] Seq=1 Ack=209 Win=30720 Len=0
328	4.810967096	192.168.2.55	107.167.110.216	TCP	60	56090 → 443 [ACK] Seq=209 Ack=2998 Win=66048 Len=0
329	4.812103436	107.167.110.216	192.168.2.55	TLSv1.2	1494	Server Hello
330	4.812114932	107.167.110.216	192.168.2.55	TLSv1.2	1494	Certificate [TCP segment of a reassembled PDU]
331	4.812126889	107.167.110.216	192.168.2.55	TLSv1.2	171	Server Key Exchange, Server Hello Done
332	4.812897166	192.168.2.55	107.167.110.216	TCP	60	56089 → 443 [ACK] Seq=209 Ack=2998 Win=66048 Len=0

Fragment offset: 0
Time to live: 57
Protocol: TCP (6)
Header checksum: 0xfcfc [validation disabled]
[Header checksum status: Unverified]
Source: 172.217.29.227
Destination: 192.168.2.55

► [Source GeoIP: United States, AS15169 Google Inc., Mountain View, CA, United States, AS15169 Google Inc., Mountain View, CA, 37.419201, -122.0574]
► [Destination GeoIP: Unknown]

```

0010  00 28 f7 3b 00 00 39 06 fc f8 ac d9 1d e3 c0 a0  .(.;.9. ....
0020  02 37 01 bb db 0d 2d 3b 5a bb 18 bc ed 40 50 10  7.....; Z...@P.
0030  00 bd b6 bf 00 00  .

```

Text item (text), 4 bytes

Packets: 520 - Displayed: 520 (100.0%) - Load time: 0:0.21 - Profile: Default

Fonte: Elaborado pelo autor, (2017)

APÊNDICE B - Resultado Teste de Minuto Com Navegação

Figura 26 – Teste de conexão ao site Moodle em um minuto com Internet Explorer

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=42881/33191, ttl=128 (reply ...)
2	0.0003635906	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=42881/33191, ttl=60 (request ...)
3	0.186518628	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
4	1.015659256	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=42882/33447, ttl=128 (reply ...)
5	1.018732114	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=42882/33447, ttl=60 (request ...)
6	1.210520834	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
7	1.292409414	192.168.2.55	192.168.2.50	DNS	77	Standard query 0x2f72 A ww.google.com.br
8	1.292458539	192.168.2.50	192.168.2.55	ICMP	105	Destination unreachable (Port unreachable)
9	1.292976228	192.168.2.55	8.8.4.4	DNS	77	Standard query 0x2f72 A ww.google.com.br
10	1.308407194	8.8.4.4	192.168.2.55	DNS	239	Standard query response 0x2f72 A ww.google.com.br A 172.217.29...
11	2.031216187	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=42883/33703, ttl=128 (reply ...)
12	2.035684508	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=42883/33703, ttl=60 (request ...)
13	2.263995107	192.168.2.55	192.168.2.50	DNS	79	Standard query 0xe698 AAAA ws12.gti.mcafee.com
14	2.264033464	192.168.2.50	192.168.2.55	ICMP	107	Destination unreachable (Port unreachable)
15	2.264039103	192.168.2.55	192.168.2.50	DNS	79	Standard query 0xb69e A ws12.gti.mcafee.com
16	2.264057856	192.168.2.50	192.168.2.55	ICMP	107	Destination unreachable (Port unreachable)
17	2.264464981	192.168.2.55	8.8.4.4	DNS	79	Standard query 0xe698 AAAA ws12.gti.mcafee.com

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: CompalIn_f4:44:4f (fc:45:96:f4:44:4f), Dst: CompalIn_0d:2d:df (20:89:84:0d:2d:df)
 Internet Protocol Version 4, Src: 192.168.2.55, Dst: 8.8.8.8
 Internet Control Message Protocol

0000 20 89 84 0d 2d df fc 45 96 f4 44 4f 08 00 45 00E..DO..E.
 0010 00 3c 67 34 00 00 00 01 00 9e c0 a8 02 37 08 08 .<g4....7..
 0020 08 08 08 00 a5 d9 00 01 a7 81 61 62 63 64 65 66<abcdef
 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

Teste Moodle IE Packets: 1900 · Displayed: 1900 (100.0%) · Load time: 0:0.59 Profile: Default

Fonte: Elaborado pelo autor, (2017)

Figura 27 – Teste de conexão ao site Moodle em um minuto com Firefox

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.55	192.16.48.200	TCP	60	53281 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2	0.000008726	192.168.2.55	192.16.48.200	TCP	60	53280 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.064248627	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43004/64679, ttl=128 (reply ...)
4	0.067229426	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43004/64679, ttl=60 (request ...)
5	0.414467746	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
6	1.080074738	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43005/64935, ttl=128 (reply ...)
7	1.083800213	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43005/64935, ttl=60 (request ...)
8	1.438468297	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
9	2.095744010	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43006/65191, ttl=128 (reply ...)
10	2.102314270	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43006/65191, ttl=60 (request ...)
11	3.112071603	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43007/65447, ttl=128 (reply ...)
12	3.115851999	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43007/65447, ttl=60 (request ...)
13	3.838459762	CompalIn_0d:2d:df	CompalIn_f4:44:4f	ARP	42	Who has 192.168.2.55? Tell 192.168.2.50
14	3.838835265	CompalIn_f4:44:4f	CompalIn_0d:2d:df	ARP	60	192.168.2.55 is at fc:45:96:f4:44:4f
15	4.127259148	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43008/168, ttl=128 (reply in...)
16	4.130815520	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43008/168, ttl=60 (request i...)
17	4.390066500	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: CompalIn_f4:44:4f (fc:45:96:f4:44:4f), Dst: CompalIn_0d:2d:df (20:89:84:0d:2d:df)
 Internet Protocol Version 4, Src: 192.168.2.55, Dst: 192.16.48.200
 Transmission Control Protocol, Src Port: 53281, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000 20 89 84 0d 2d df fc 45 96 f4 44 4f 08 00 45 00E..DO..E.
 0010 08 28 13 50 40 00 00 06 33 c8 c0 a8 02 37 c0 10 (.P8... 3...7..
 0020 3c c8 d0 21 01 bb f8 7f 6c c9 70 eb bd b0 50 14 0..l...l.p...P.

Teste Moodle Firefox Packets: 1349 · Displayed: 1349 (100.0%) · Load time: 0:0.36 Profile: Default

Fonte: Elaborado pelo autor, (2017)

Figura 28 – Teste de conexão ao site Moodle em um minuto com Chrome

No.	Time	Source	Destination	Protocol	Length	Info
27	3.623057716	192.168.2.55	172.217.29.227	TCP	66	53178 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM...
28	3.624012298	192.168.2.55	172.217.29.227	TCP	66	53179 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM...
29	3.653041814	172.217.29.227	192.168.2.55	TCP	66	80 → 53178 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK...
30	3.653102229	192.168.2.55	172.217.29.227	TCP	60	53178 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
31	3.654215299	192.168.2.55	172.217.29.227	HTTP	457	GET / HTTP/1.1
32	3.654508790	172.217.29.227	192.168.2.55	TCP	66	80 → 53179 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK...
33	3.654937267	192.168.2.55	172.217.29.227	TCP	60	53179 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
34	3.683098984	172.217.29.227	192.168.2.55	TCP	54	80 → 53178 [ACK] Seq=1 Ack=404 Win=44032 Len=0
35	3.737039558	172.217.29.227	192.168.2.55	HTTP	600	HTTP/1.1 301 Moved Permanently (text/html)
36	3.743523032	192.168.2.55	192.168.2.50	DNS	77	Standard query 0x687c A www.google.com.br
37	3.743567184	192.168.2.50	192.168.2.55	ICMP	105	Destination unreachable (Port unreachable)
38	3.744518134	192.168.2.55	8.8.4.4	DNS	77	Standard query 0x687c A www.google.com.br
39	3.749970292	8.8.4.4	192.168.2.55	DNS	239	Standard query response 0x687c A www.google.com.br A 172.217.29...
40	3.752435283	192.168.2.55	172.217.29.227	TCP	66	53180 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM...
41	3.753095468	192.168.2.55	172.217.29.227	TCP	66	53181 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM...
42	3.767588931	192.168.2.55	192.168.2.50	DNS	84	Standard query 0x68b2 A translate.googleapis.com
43	3.767632412	192.168.2.50	192.168.2.55	ICMP	105	Destination unreachable (Port unreachable)
44	3.767638750	192.168.2.55	192.168.2.50	DNS	89	Standard query 0x9579 A client-services.googleapis.com

Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0x5962 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.2.55
 Destination: 172.217.29.227
 [Source GeoIP: Unknown]
 [Destination GeoIP: United States, AS15169 Google Inc., Mountain View, CA, United States, AS15169 Google Inc., Mountain View, CA, 37.419201, -122...]
 Transmission Control Protocol, Src Port: 53180, Dst Port: 80, Seq: 0, Len: 0

0900 20 89 84 0d 2d df fc 45 96 f4 44 4f 08 00 45 00E..D0..E.
 0910 00 34 13 c6 40 00 80 06 59 62 c0 a8 02 37 08 08 .4..@...YB...7..
 0920 1d e3 cf bc 00 50 e7 e4 5f 7f 00 00 00 00 80 02P...

Fonte: Elaborado pelo autor, (2017)

Figura 29 – Teste de conexão ao site Moodle um minuto com Edge

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43403/35753, ttl=128 (reply ...)
2	0.003441405	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43403/35753, ttl=60 (request...)
3	0.638672097	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
4	1.015764818	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43404/36009, ttl=128 (reply ...)
5	1.019309367	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43404/36009, ttl=60 (request...)
6	1.039075189	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
7	2.031236721	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43405/36265, ttl=128 (reply ...)
8	2.034618708	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43405/36265, ttl=60 (request...)
9	2.328447255	192.168.2.55	172.217.29.227	TCP	66	53527 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
10	2.328518911	192.168.2.55	172.217.29.227	TCP	66	53528 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
11	2.357048974	172.217.29.227	192.168.2.55	TCP	66	80 → 53527 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK...
12	2.357062414	172.217.29.227	192.168.2.55	TCP	66	80 → 53528 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK...
13	2.357511638	192.168.2.55	172.217.29.227	TCP	60	53527 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
14	2.357530402	192.168.2.55	172.217.29.227	TCP	60	53528 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
15	2.357801512	192.168.2.55	172.217.29.227	HTTP	374	GET / HTTP/1.1
16	2.387955619	172.217.29.227	192.168.2.55	TCP	54	80 → 53528 [ACK] Seq=1 Ack=321 Win=44032 Len=0
17	2.389080413	192.168.2.55	104.41.62.122	TCP	66	53529 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: CompalIn_f4:44:4f (fc:45:96:f4:44:4f), Dst: CompalIn_0d:2d:df (20:89:84:0d:2d:df)
 Internet Protocol Version 4, Src: 192.168.2.55, Dst: 8.8.8.8
 Internet Control Message Protocol

0900 20 89 84 0d 2d df fc 45 96 f4 44 4f 08 00 45 00E..D0..E.
 0910 00 3c 09 b9 00 00 80 01 fe 18 c0 a8 02 37 08 08 .<1.....7..
 0920 08 08 08 00 a3 cf 00 01 a9 8b 61 62 63 64 65 66abcdef
 0930 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

Fonte: Elaborado pelo autor, (2017)

Figura 30 – Teste de conexão ao site Moodle em um minuto com Opera

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43129/31144, ttl=60
2	0.163273527	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
3	0.822099178	Compalln_f4:44:4f	Compalln_0d:2d:df	ARP	60	Who has 192.168.2.50? Tell 192.168.2.55
4	0.822118395	Compalln_0d:2d:df	Compalln_f4:44:4f	ARP	42	192.168.2.50 is at 20:89:84:0d:2d:df
5	1.009893177	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43130/31400, ttl=128 (reply ...)
6	1.013226425	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43130/31400, ttl=60 (request ...)
7	2.025637764	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43131/31656, ttl=128 (reply ...)
8	2.033973140	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43131/31656, ttl=60 (request ...)
9	3.041478995	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43132/31912, ttl=128 (reply ...)
10	3.047990415	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43132/31912, ttl=60 (request ...)
11	3.136947933	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
12	3.395904120	192.168.2.55	8.8.4.4	DNS	74	Standard query 0x58a9 A www.google.com
13	3.396930360	192.168.2.55	192.168.2.255	NBNS	92	Name query NB WPAD-00>
14	3.397451159	fe80::cdae:fdd3:a97...	ff02::1:3	LLMNR	84	Standard query 0x30bb A wpad
15	3.397707356	192.168.2.55	224.0.0.252	LLMNR	64	Standard query 0x30bb A wpad
16	3.402434342	8.8.4.4	192.168.2.55	DNS	226	Standard query response 0x58a9 A www.google.com A 172.217.29.228...
17	3.807127050	fe80::cdae:fdd3:a97...	ff02::1:3	LLMNR	84	Standard query 0x30bb A wpad

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: Compalln_0d:2d:df (20:89:84:0d:2d:df), Dst: Compalln_f4:44:4f (fc:45:96:f4:44:4f)
 Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.2.55
 Internet Control Message Protocol

0000 ff ff ff ff ff ff 20 89 84 0d 2d df 00 00 00 00
 0010 00 3c d6 57 00 00 3c 01 d5 7a 08 08 08 c0 a8
 0020 02 37 00 00 ac e1 00 01 a8 79 61 62 63 64 65 66
 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76

Packets: 1896 · Displayed: 1896 (100.0%) · Load time: 0:0.74 Profile: Default

Fonte: Elaborado pelo autor, (2017)

Figura 31 – Teste de conexão ao site Inf Passo Fundo em um minuto com Internet Explorer

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
2	0.221267492	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43539/5034, ttl=128 (reply i...)
3	0.224660207	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43539/5034, ttl=60 (request ...)
4	1.237046947	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43540/5290, ttl=128 (reply i...)
5	1.240234280	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43540/5290, ttl=60 (request ...)
6	1.529035501	192.168.2.55	192.168.2.50	DNS	77	Standard query 0x4ee1 A www.google.com.br
7	1.529080189	192.168.2.50	192.168.2.55	ICMP	105	Destination unreachable (Port unreachable)
8	1.529084430	192.168.2.55	8.8.4.4	DNS	77	Standard query 0x4ee1 A www.google.com.br
9	1.538433500	8.8.4.4	192.168.2.55	DNS	239	Standard query response 0x4ee1 A www.google.com.br A 172.217.29...
10	2.252472313	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43541/5546, ttl=128 (reply i...)
11	2.255446862	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43541/5546, ttl=60 (request ...)
12	2.429379553	192.168.2.55	192.168.2.50	DNS	79	Standard query 0x044d AAAA ws12.gti.mcafee.com
13	2.429425591	192.168.2.50	192.168.2.55	ICMP	107	Destination unreachable (Port unreachable)
14	2.429431053	192.168.2.55	192.168.2.50	DNS	79	Standard query 0x44a9 A ws12.gti.mcafee.com
15	2.429449000	192.168.2.50	192.168.2.55	ICMP	107	Destination unreachable (Port unreachable)
16	2.429901050	192.168.2.55	8.8.4.4	DNS	79	Standard query 0x44a9 A ws12.gti.mcafee.com
17	2.429903260	192.168.2.55	8.8.4.4	DNS	78	Standard query 0x044d AAAA ws12.gti.mcafee.com

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 Ethernet II, Src: Compalln_0d:2d:df (20:89:84:0d:2d:df), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 20 89 84 0d 2d df 00 00 00 01
 0010 00 00 06 04 00 01 20 89 84 0d 2d df c0 a8 02 32
 0020 00 00 00 00 00 00 c0 a8 02 01

Packets: 5600 · Displayed: 5600 (100.0%) · Load time: 0:0.204 Profile: Default

Fonte: Elaborado pelo autor, (2017)

Figura 32 – Teste de conexão ao site Inf Passo Fundo em um minuto com Firefox

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=44063/8108, ttl=128 (reply i...
2	0.003737933	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=44063/8108, ttl=60 (request ...
3	0.336866714	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
4	1.015719934	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=44064/8364, ttl=128 (reply i...
5	1.225033948	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=44064/8364, ttl=60 (request ...
6	1.369866771	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
7	2.031371940	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=44065/8620, ttl=128 (reply i...
8	3.104554947	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=44065/8620, ttl=60 (request ...
9	3.107003498	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=44066/8876, ttl=128 (reply i...
10	3.764414827	192.168.2.55	192.168.2.50	DNS	84	Standard query 0xf173 A detectportal.firefox.com
11	3.764414810	192.168.2.55	192.168.2.55	ICMP	112	Destination unreachable (Port unreachable)
12	3.764382850	192.168.2.55	8.8.4.4	DNS	84	Standard query 0xf173 A detectportal.firefox.com
13	3.859424299	192.168.2.55	192.168.2.50	DNS	73	Standard query 0x3817 A google.com.br
14	3.859451081	192.168.2.50	192.168.2.55	ICMP	101	Destination unreachable (Port unreachable)
15	3.860020078	192.168.2.55	8.8.4.4	DNS	73	Standard query 0x3817 A google.com.br
16	4.021567831	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
17	4.254264510	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=44066/8876, ttl=60 (request ...

▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 ▶ Ethernet II, Src: Compalln_f4:44:4f (fc:45:96:f4:44:4f), Dst: Compalln_0d:2d:df (20:89:84:0d:2d:df)
 ▶ Internet Protocol Version 4, Src: 192.168.2.55, Dst: 8.8.8.8
 ▶ Internet Control Message Protocol

0000 20 89 84 0d 2d df fc 45 96 f4 44 4f 08 00 45 00E..DO..E.
 0010 00 3c 6c e1 00 00 80 01 fa f0 c0 a8 02 37 08 08 ..<1.....7..
 0020 08 08 00 00 a1 3b 00 01 ac 1f 61 62 63 64 65 66:..abcdef
 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn oppqrstuv
 0040 77 61 62 63 64 65 66 67 68 69 wabcedfg hi

Teste Inf Firefox Packets: 4997 · Displayed: 4997 (100.0%) · Load time: 0:0.221 Profile: Default

Fonte: Elaborado pelo autor, (2017)

Figura 33 – Teste de conexão ao site Inf Passo Fundo em um minuto com Chrome

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
2	0.160880702	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43951/44971, ttl=128 (reply ...
3	0.166707291	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43951/44971, ttl=60 (request ...
4	1.119993905	Compalln_0d:2d:df	Compalln_f4:44:4f	ARP	42	Who has 192.168.2.55? Tell 192.168.2.50
5	1.121439755	Compalln_f4:44:4f	Compalln_0d:2d:df	ARP	60	192.168.2.55 is at fc:45:96:f4:44:4f
6	1.176421280	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43952/45227, ttl=128 (reply ...
7	1.179478575	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43952/45227, ttl=60 (request ...
8	2.192362127	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43953/45483, ttl=128 (reply ...
9	2.195536665	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43953/45483, ttl=60 (request ...
10	2.960486918	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
11	3.193201161	192.168.2.55	192.168.2.255	NBNS	92	Name query NB WPAD<00>
12	3.194068482	fe80::cdae:fdd3:a97...	ff02::1:3	LLMNR	84	Standard query 0x1795 A wpad
13	3.194383916	192.168.2.55	224.0.0.252	LLMNR	64	Standard query 0x1795 A wpad
14	3.212953030	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=43954/45739, ttl=128 (reply ...
15	3.216427196	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=43954/45739, ttl=60 (request ...
16	3.369680468	192.168.2.55	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
17	3.369879512	fe80::cdae:fdd3:a97...	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question

▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 ▶ Ethernet II, Src: Compalln_0d:2d:df (20:89:84:0d:2d:df), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 20 89 84 0d 2d df 08 06 00 01:.....
 0010 08 00 06 04 00 01 20 89 84 0d 2d df c0 a8 02 32:.....2
 0020 00 00 00 00 00 c0 a8 02 01:.....

Teste Inf Chrome Packets: 4489 · Displayed: 4489 (100.0%) · Load time: 0:0.178 Profile: Default

Fonte: Elaborado pelo autor, (2017)

Figura 34 – Teste de conexão ao site Inf Passo Fundo em um minuto com Edge

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=44282/64172, ttl=128 (reply ...)
2	0.003158170	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=44282/64172, ttl=60 (request ...)
3	1.015907749	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=44283/64428, ttl=128 (reply ...)
4	1.019201092	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=44283/64428, ttl=60 (request ...)
5	1.709456567	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
6	1.912817258	192.168.2.55	192.168.2.50	DNS	73	Standard query 0x3ea2 A google.com.br
7	1.912858711	192.168.2.50	192.168.2.55	DNS	101	Destination unreachable (Port unreachable)
8	1.913299927	192.168.2.55	8.8.4.4	DNS	73	Standard query 0x3ea2 A google.com.br
9	1.922686871	8.8.4.4	192.168.2.55	DNS	235	Standard query response 0x3ea2 A google.com.br A 172.217.29.227 ...
10	1.966489882	192.168.2.55	172.217.29.227	TCP	66	54167 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
11	1.966530357	192.168.2.55	172.217.29.227	TCP	66	54166 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
12	1.992251832	172.217.29.227	192.168.2.55	TCP	66	80 → 54167 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK...
13	1.992638421	192.168.2.55	172.217.29.227	TCP	66	54167 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
14	1.992886726	172.217.29.227	192.168.2.55	TCP	66	80 → 54166 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK...
15	1.992903427	192.168.2.55	172.217.29.227	HTTP	374	GET / HTTP/1.1
16	1.993282325	192.168.2.55	172.217.29.227	TCP	60	54166 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
17	2.024193373	172.217.29.227	192.168.2.55	TCP	54	80 → 54167 [ACK] Seq=1 Ack=321 Win=44032 Len=0

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: Compalln_f4:44:4f (fc:45:96:f4:44:4f), Dst: Compalln_0d:2d:df (20:89:84:0d:2d:df)
 Internet Protocol Version 4, Src: 192.168.2.55, Dst: 8.8.8.8
 Internet Control Message Protocol

0000 20 89 84 0d 2d df fc 45 96 f4 44 4f 08 00 45 00E..D0..E.
 0010 00 3c 6e 35 00 00 80 01 f9 9c c0 a8 02 37 08 08 .<n5.....7..
 0020 08 08 08 00 a0 60 00 01 ac fa 61 62 63 64 65 66abcdef
 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

Teste Inf Edge Packets: 6072 · Displayed: 6072 (100.0%) · Load time: 0:0.218 Profile: Default

Fonte: Elaborado pelo autor, (2017)

Figura 35 – Teste de conexão ao site Inf Passo Fundo em um minuto com Opera

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=44166/34476, ttl=128 (reply ...)
2	0.003520084	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=44166/34476, ttl=60 (request ...)
3	1.015748662	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=44167/34732, ttl=128 (reply ...)
4	1.019088534	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=44167/34732, ttl=60 (request ...)
5	2.031536864	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=44168/34988, ttl=128 (reply ...)
6	2.034912693	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=44168/34988, ttl=60 (request ...)
7	2.094958515	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
8	2.817119873	192.168.2.55	192.168.2.255	NBNS	92	Name query NB WPAD<0>
9	2.817159523	192.168.2.55	192.168.2.50	DNS	74	Standard query 0xcfff A www.google.com
10	2.817197051	192.168.2.50	192.168.2.55	ICMP	102	Destination unreachable (Port unreachable)
11	2.817410732	fe80::cdae:fdd3:a97... ffd3:1:3	LLMNR	84	Standard query 0x76de A wpad	
12	2.817653628	192.168.2.55	8.8.4.4	DNS	74	Standard query 0xcfff A www.google.com
13	2.817701523	192.168.2.55	224.0.0.252	LLMNR	64	Standard query 0x76de A wpad
14	2.827244086	8.8.4.4	192.168.2.55	DNS	226	Standard query response 0xcfff A www.google.com A 172.217.29.228...
15	3.047222142	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=44169/35244, ttl=128 (reply ...)
16	3.057163855	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=44169/35244, ttl=60 (request ...)

Frame 10: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
 Ethernet II, Src: Compalln_0d:2d:df (20:89:84:0d:2d:df), Dst: Compalln_f4:44:4f (fc:45:96:f4:44:4f)
 Internet Protocol Version 4, Src: 192.168.2.50, Dst: 192.168.2.55
 Internet Control Message Protocol

0000 fc 45 96 f4 44 4f 20 89 84 0d 2d df 08 00 45 c0 .E..D0.E.
 0010 00 58 c6 af 00 00 40 01 2d 7c c0 a8 02 32 c0 a8 .X....@. -|...2..
 0020 02 37 03 03 82 f0 00 00 00 09 45 00 00 3c 65 6a .7.....E.<ej
 0030 00 00 00 11 4f 8d c0 a8 02 37 c0 a8 02 32 c7 1c0....7...2..
 0040 00 35 00 28 53 eb cf ff 01 00 00 01 00 00 00 00 .5.(S.....

Teste Inf Opera Packets: 4590 · Displayed: 4590 (100.0%) · Load time: 0:0.192 Profile: Default

Fonte: Elaborado pelo autor, (2017)

Figura 36 – Teste de conexão ao site Americanas em um minuto com Internet Explorer

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=45183/32688, ttl=60
2	0.049370724	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
3	0.739603891	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=45184/32944, ttl=128 (reply ...)
4	0.744772129	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=45184/32944, ttl=60 (request ...)
5	1.151493452	192.168.2.55	192.168.2.50	DNS	77	Standard query 0x85ef A www.google.com.br
6	1.151539573	192.168.2.50	192.168.2.55	ICMP	105	Destination unreachable (Port unreachable)
7	1.152055923	192.168.2.55	8.8.4.4	DNS	77	Standard query 0x85ef A www.google.com.br
8	1.157381196	8.8.4.4	192.168.2.55	DNS	239	Standard query response 0x85ef A www.google.com.br A 172.217.29...
9	1.524886213	192.168.2.55	172.217.29.227	TCP	66	54569 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
10	1.524965746	192.168.2.55	172.217.29.227	TCP	66	54570 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
11	1.553311887	172.217.29.227	192.168.2.55	TCP	66	443 → 54569 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK...
12	1.553356991	172.217.29.227	192.168.2.55	TCP	66	443 → 54570 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK...
13	1.553692806	192.168.2.55	172.217.29.227	TCP	60	54569 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
14	1.553734868	192.168.2.55	172.217.29.227	TCP	60	54570 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
15	1.556275647	192.168.2.55	172.217.29.227	TLSv1.2	260	Client Hello
16	1.556369176	192.168.2.55	172.217.29.227	TLSv1.2	260	Client Hello

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: CompalIn_0d:2d:df (20:89:84:0d:2d:df), Dst: CompalIn_f4:44:4f (fc:45:96:f4:44:4f)
 Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.2.55
 Internet Control Message Protocol

0000 fc 45 96 f4 44 4f 20 89 84 0d 2d df 08 00 45 00 .E..DO...E.
 0010 00 3c eb 21 00 00 3c 01 c0 b9 08 08 08 08 c0 a8 <.!...<.....
 0020 02 37 00 00 a4 db 00 01 b0 7f 61 62 63 64 65 66 .7.....!..abcdef
 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmnopqrstuv
 0040 77 61 62 63 64 65 66 67 68 69 wabcdfgh

Fonte: Elaborado pelo autor, (2017)

Figura 37 – Teste de conexão ao site Americanas em um minuto com Firefox

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=45543/59313, ttl=128 (reply ...)
2	0.003632254	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=45543/59313, ttl=60 (request ...)
3	1.015819526	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=45544/59569, ttl=128 (reply ...)
4	1.020299496	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=45544/59569, ttl=60 (request ...)
5	1.326579819	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
6	2.031312389	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=45545/59825, ttl=128 (reply ...)
7	2.035599455	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=45545/59825, ttl=60 (request ...)
8	2.355281806	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
9	2.597590809	192.168.2.55	192.168.2.50	DNS	84	Standard query 0x4520 A detectportal.firefox.com
10	2.597644185	192.168.2.50	192.168.2.55	ICMP	105	Destination unreachable (Port unreachable)
11	2.598194814	192.168.2.55	8.8.4.4	DNS	84	Standard query 0x4520 A detectportal.firefox.com
12	2.603805531	8.8.4.4	192.168.2.55	DNS	515	Standard query response 0x4520 A detectportal.firefox.com CNAME ...
13	2.607470760	192.168.2.55	186.208.80.71	TCP	66	55111 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM...
14	2.612693655	186.208.80.71	192.168.2.55	TCP	66	80 → 55111 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK...
15	2.613099835	192.168.2.55	186.208.80.71	TCP	60	55111 → 80 [ACK] Seq=1 Ack=1 Win=66948 Len=0
16	2.613344920	192.168.2.55	186.208.80.71	HTTP	373	GET /success.txt HTTP/1.1

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: CompalIn_f4:44:4f (fc:45:96:f4:44:4f), Dst: CompalIn_0d:2d:df (20:89:84:0d:2d:df)
 Internet Protocol Version 4, Src: 192.168.2.55, Dst: 8.8.8.8
 Internet Control Message Protocol

0000 20 89 84 0d 2d df fc 45 96 f4 44 4f 08 00 45 00E..DO.E.
 0010 00 3c 75 5a 00 00 00 01 f2 77 c0 a8 02 37 08 08 <uZ....w..7..
 0020 08 08 08 00 9b 73 00 01 b1 e7 61 62 63 64 65 66s...!..abcdef
 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmnopqrstuv
 0040 77 61 62 63 64 65 66 67 68 69 wabcdfgh

Fonte: Elaborado pelo autor, (2017)

Figura 38 – Teste de conexão ao site Americanas em um minuto com Chrome

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	CompalIn_f4:44:4f	CompalIn_0d:2d:df	ARP	60	Who has 192.168.2.50? Tell 192.168.2.55
2	0.000018312	CompalIn_0d:2d:df	CompalIn_f4:44:4f	ARP	42	192.168.2.50 is at 20:89:84:0d:2d:df
3	0.297285290	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=45296/61616, ttl=128 (reply ...)
4	0.388302774	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=45296/61616, ttl=60 (request...)
5	0.525683398	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
6	1.312977070	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=45297/61872, ttl=128 (reply ...)
7	1.446508964	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=45297/61872, ttl=60 (request...)
8	2.328606389	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=45298/62128, ttl=128 (reply ...)
9	2.614422227	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=45298/62128, ttl=60 (request...)
10	3.344348296	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=45299/62384, ttl=128 (reply ...)
11	3.420651470	192.168.2.55	192.168.2.50	DNS	75	Standard query 0xc82c A apis.google.com
12	3.420698496	192.168.2.50	192.168.2.55	ICMP	103	Destination unreachable (Port unreachable)
13	3.421288776	192.168.2.55	8.8.4.4	DNS	75	Standard query 0xc82c A apis.google.com
14	3.421767700	192.168.2.55	192.168.2.50	DNS	73	Standard query 0x862c A google.com.br
15	3.421790920	192.168.2.50	192.168.2.55	ICMP	101	Destination unreachable (Port unreachable)
16	3.42322673	192.168.2.55	192.168.2.50	DNS	75	Standard query 0xda1f A ssl.gstatic.com

Fonte: Elaborado pelo autor, (2017)

Figura 39 – Teste de conexão ao site Americanas em um minuto com Edge

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.55	64.4.54.254	TCP	60	55662 → 443 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
2	0.000070125	192.168.2.55	65.55.44.108	TCP	60	55663 → 443 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
3	0.059591364	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
4	0.156634171	65.55.44.108	192.168.2.55	TCP	54	443 → 55663 [FIN, ACK] Seq=1 Ack=2 Win=513 Len=0
5	0.157853241	192.168.2.55	65.55.44.108	TCP	60	55663 → 443 [ACK] Seq=2 Ack=2 Win=257 Len=0
6	0.187527181	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=46896/12471, ttl=128 (reply ...)
7	0.189829107	64.4.54.254	192.168.2.55	TCP	54	443 → 55662 [FIN, ACK] Seq=1 Ack=2 Win=1024 Len=0
8	0.190575697	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=46896/12471, ttl=60 (request...)
9	0.191041813	192.168.2.55	64.4.54.254	TCP	60	55662 → 443 [ACK] Seq=2 Ack=2 Win=256 Len=0
10	1.059290671	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
11	1.203441328	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=46897/12727, ttl=128 (reply ...)
12	1.206497147	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=46897/12727, ttl=60 (request...)
13	2.083298491	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
14	2.218763992	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=46898/12983, ttl=128 (reply ...)
15	2.221866316	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=46898/12983, ttl=60 (request...)
16	3.128230927	192.168.2.55	192.168.2.50	DNS	73	Standard query 0x9ebb A google.com.br

Fonte: Elaborado pelo autor, (2017)

Figura 40 – Teste de conexão ao site Americanas em um minuto com Chrome

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
2	0.877891529	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=46758/42678, ttl=128 (reply ...)
3	0.882522789	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=46758/42678, ttl=60 (request...)
4	1.014669165	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
5	1.565235181	192.168.2.55	68.67.180.45	TCP	60	55484 → 443 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
6	1.893583192	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=46759/42934, ttl=128 (reply ...)
7	1.897017234	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=46759/42934, ttl=60 (request...)
8	2.030667348	Compalln_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
9	2.731573608	192.168.2.55	192.168.2.255	NBNS	92	Name query NB WPAD=00>
10	2.732059685	fe80::cdae:fdd3:a97...	ff02::1:3	LLMNR	84	Standard query 0xd47c A wpad
11	2.732277021	192.168.2.55	224.0.0.252	LLMNR	64	Standard query 0xd47c A wpad
12	2.913628680	192.168.2.55	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=46760/43190, ttl=128 (reply ...)
13	2.917725980	8.8.8.8	192.168.2.55	ICMP	74	Echo (ping) reply id=0x0001, seq=46760/43190, ttl=60 (request...)
14	3.131865253	fe80::cdae:fdd3:a97...	ff02::1:3	LLMNR	84	Standard query 0xd47c A wpad
15	3.132012516	192.168.2.55	224.0.0.252	LLMNR	64	Standard query 0xd47c A wpad
16	3.300583993	104.20.17.50	192.168.2.55	TCP	54	80 → 55476 [FIN, ACK] Seq=1 Ack=1 Win=30 Len=0

▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 ▶ Ethernet II, Src: Compalln_0d:2d:df (20:89:84:0d:2d:df), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Address Resolution Protocol (request)

```

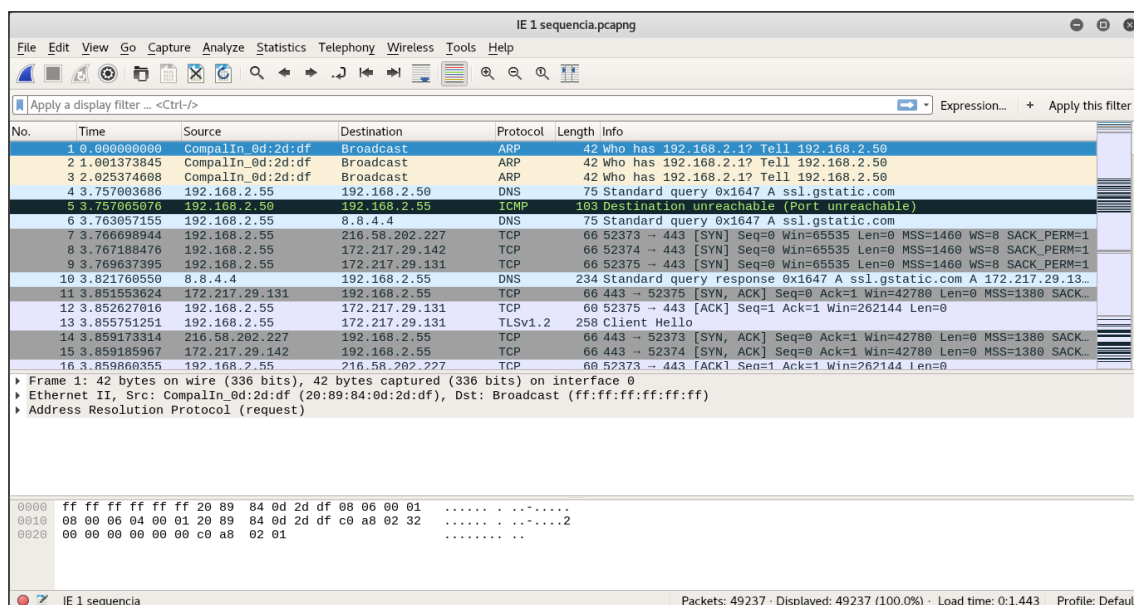
0000  ff ff ff ff ff ff 20 89 84 0d 2d df 08 06 00 01  .....:..:....
0010  08 00 06 04 00 01 20 89 84 0d 2d df c0 a8 02 32  .....:..:....2
0020  00 00 00 00 00 00 c0 a8 02 01  .....:
  
```

Teste Compras Opera Packets: 13498 · Displayed: 13498 (100.0%) · Load time: 0:0.370 Profile: Default

Fonte: Elaborado pelo autor, (2017)

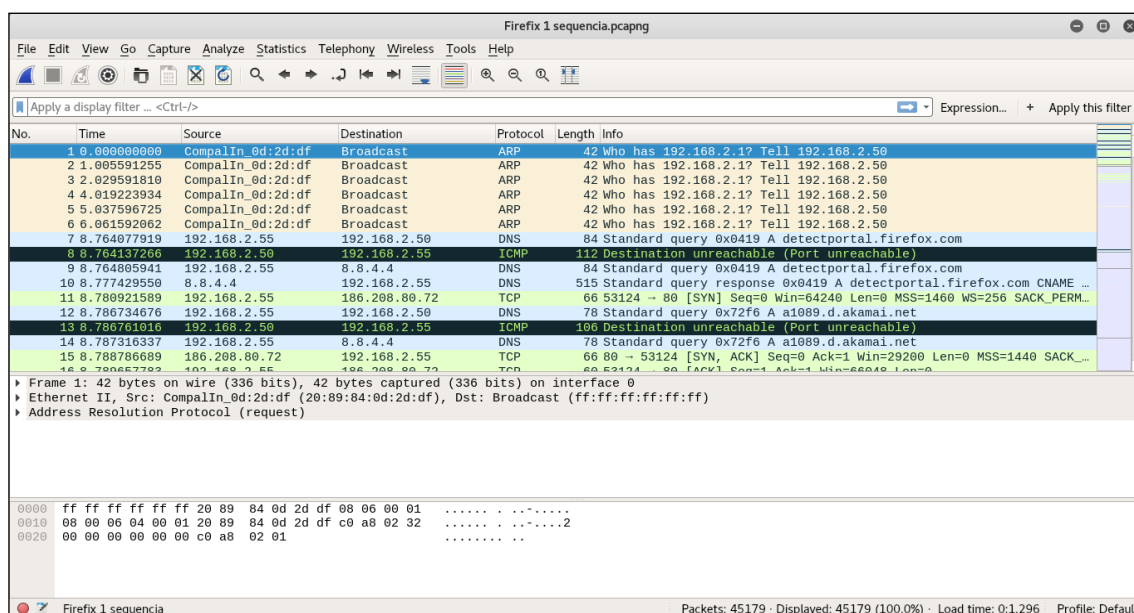
APÊNDICE C - Resultado Teste de Completo de Navegação

Figura 41 – Teste completo de conexão com Internet Explorer



Fonte: Elaborado pelo autor, (2017)

Figura 42 – Teste completo de conexão com Firefox



Fonte: Elaborado pelo autor, (2017)

Figura 43 – Teste completo de conexão com Chrome

Chrome 1 sequencia.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + Apply this filter

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
2	1.005207291	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
3	2.029205992	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
4	5.484103366	192.168.2.55	192.168.2.255	NBNS	92	Name query NB WPAD<00>
5	5.484900974	fe80::cdae:fdd3:a97...	ff02::1:3	LLMNR	84	Standard query 0xdcac A wpad
6	5.485366465	192.168.2.55	224.0.0.252	LLMNR	64	Standard query 0xdcac A wpad
7	5.635318764	192.168.2.55	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
8	5.635597816	fe80::cdae:fdd3:a97...	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
9	5.685676405	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
10	5.895602289	fe80::cdae:fdd3:a97...	ff02::1:3	LLMNR	84	Standard query 0xdcac A wpad
11	5.895657090	192.168.2.55	224.0.0.252	LLMNR	64	Standard query 0xdcac A wpad
12	6.113063563	192.168.2.55	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
13	6.144981231	192.168.2.55	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
14	6.145026437	fe80::cdae:fdd3:a97...	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
15	6.145770700	192.168.2.55	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
16	6.145804944	fe80::cdae:fdd3:a97...	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 Ethernet II, Src: CompalIn_0d:2d:df (20:89:84:0d:2d:df), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request)

```

0000 ff ff ff ff ff ff 20 89 84 0d 2d df 08 06 00 01 .....
0010 08 00 06 04 00 01 20 89 84 0d 2d df c0 a8 02 32 .....2
0020 00 00 00 00 00 00 c0 a8 02 01 .....

```

Chrome 1 sequencia Packets: 40332 · Displayed: 40332 (100.0%) · Load time: 0:1.0 Profile: Default

Fonte: Elaborado pelo autor, (2017)

Figura 44 – Teste completo de conexão com Edge

Edge 1 sequencia.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + Apply this filter

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
2	2.969803967	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
3	4.000002299	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
4	5.024003522	CompalIn_0d:2d:df	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.50
5	6.025411508	192.168.2.55	192.168.2.50	DNS	84	Standard query 0x0c8d A sls.update.microsoft.com
6	6.025467515	192.168.2.50	192.168.2.55	ICMP	112	Destination unreachable (Port unreachable)
7	6.026100346	192.168.2.55	8.8.4.4	DNS	84	Standard query 0x0c8d A sls.update.microsoft.com
8	6.632353520	8.8.4.4	192.168.2.55	DNS	423	Standard query response 0x0c8d A sls.update.microsoft.com CNAME ...
9	6.633738251	192.168.2.55	157.56.77.140	TCP	66	53723 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER...
10	6.703045174	192.168.2.55	172.217.29.131	TCP	60	53724 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
11	6.703075900	192.168.2.55	172.217.29.131	TCP	66	53725 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
12	6.732114742	172.217.29.131	192.168.2.55	TCP	66	80 → 53724 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK_...
13	6.732132298	172.217.29.131	192.168.2.55	TCP	66	80 → 53725 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK_...
14	6.732591459	192.168.2.55	172.217.29.131	TCP	60	53724 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
15	6.732633247	192.168.2.55	172.217.29.131	TCP	60	53725 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
16	6.732826848	192.168.2.55	172.217.29.131	HTTP	374	GET / HTTP/1.1

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 Ethernet II, Src: CompalIn_0d:2d:df (20:89:84:0d:2d:df), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request)

```

0000 ff ff ff ff ff ff 20 89 84 0d 2d df 08 06 00 01 .....
0010 08 00 06 04 00 01 20 89 84 0d 2d df c0 a8 02 32 .....2
0020 00 00 00 00 00 00 c0 a8 02 01 .....

```

Edge 1 sequencia Packets: 49770 · Displayed: 49770 (100.0%) · Load time: 0:1.556 Profile: Default

Fonte: Elaborado pelo autor, (2017)

Figura 45 – Teste completo de conexão com Opera

Opera 1 sequencia.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + Apply this filter

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	CompalIn_0d:2d:df	Broadcast	ARP	42	who has 192.168.2.1? Tell 192.168.2.50
2	1.031547194	CompalIn_0d:2d:df	Broadcast	ARP	42	who has 192.168.2.1? Tell 192.168.2.50
3	2.055547087	CompalIn_0d:2d:df	Broadcast	ARP	42	who has 192.168.2.1? Tell 192.168.2.50
4	4.909530081	192.168.2.55	192.168.2.255	NBNS	92	Name query NB WPAD<00>
5	4.910173394	fe80::cdae:fdd3:a97...	ff02::1:3	LLMNR	84	Standard query 0x1c05 A wpad
6	4.910474312	192.168.2.55	224.0.0.252	LLMNR	64	Standard query 0x1c05 A wpad
7	5.005072509	CompalIn_0d:2d:df	Broadcast	ARP	42	who has 192.168.2.1? Tell 192.168.2.50
8	5.317951747	fe80::cdae:fdd3:a97...	ff02::1:3	LLMNR	84	Standard query 0x1c05 A wpad
9	5.318189779	192.168.2.55	224.0.0.252	LLMNR	64	Standard query 0x1c05 A wpad
10	5.653812559	192.168.2.55	192.168.2.255	NBNS	92	Name query NB WPAD<00>
11	5.903940309	192.168.2.55	192.168.2.50	DNS	74	Standard query 0x2a39 A duckduckgo.com
12	5.909030780	192.168.2.50	192.168.2.55	ICMP	102	Destination unreachable (Port unreachable)
13	5.909013161	192.168.2.55	192.168.2.50	DNS	76	Standard query 0x89e1 A search.yahoo.com
14	5.909030908	192.168.2.50	192.168.2.55	ICMP	104	Destination unreachable (Port unreachable)
15	5.909033915	192.168.2.55	192.168.2.50	DNS	77	Standard query 0x0377 A www.wikipedia.org

▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 ▶ Ethernet II, Src: CompalIn_0d:2d:df (20:89:84:0d:2d:df), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff 20 89 84 0d 2d df 08 06 00 01  .....
0010  08 00 06 04 00 01 20 89 84 0d 2d df c0 a8 02 32  .....2
0020  00 00 00 00 00 00 c0 a8 02 01  .....
  
```

Opera 1 sequencia Packets: 42684 · Displayed: 42684 (100.0%) · Load time: 0:1.238 Profile: Default

Fonte: Elaborado pelo autor, (2017)