

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ  
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO  
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA  
CURSO DE ESPECIALIZAÇÃO EM REDES DE COMPUTADORES E  
TELEINFORMÁTICA

MARIO LOBO ROMERO

**IMPLEMENTAÇÃO DE UM DISPOSITIVO PORTÁTIL DE  
ROTEAMENTO PARA REDES ANÔNIMAS BASEADO EM  
RASPBERRY PI**

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA  
2018

MARIO LOBO ROMERO

**IMPLEMENTAÇÃO DE UM DISPOSITIVO PORTÁTIL DE  
ROTEAMENTO PARA REDES ANÔNIMAS BASEADO EM  
RASPBERRY PI**

Monografia de Especialização, apresentada ao Curso de Especialização em Redes de Computadores e Teleinformática, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Esp. Douglas Eduardo Basso

CURITIBA  
2018



Ministério da Educação  
Universidade Tecnológica Federal do Paraná  
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação  
Departamento Acadêmico de Eletrônica  
Curso de Especialização em Redes de Computadores e  
Teleinformática



---

## TERMO DE APROVAÇÃO

### IMPLEMENTAÇÃO DE UM DISPOSITIVO PORTÁTIL DE ROTEAMENTO PARA REDES ANÔNIMAS BASEADO EM RASPBERRY PI

por

MARIO LOBO ROMERO

Esta Monografia foi apresentada em 25 de Novembro de 2018 como requisito parcial para a obtenção do título de Especialista em Redes de Computadores e Teleinformática. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

---

Prof. Esp. Douglas Eduardo Basso  
Orientador

---

Prof. Dr. Kleber Kendy Horikawa Nabas  
Membro titular

---

Prof. M.Sc. Omero Francisco Bertol  
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho a minha família,  
pelos momentos de ausência.

## **AGRADECIMENTOS**

Agradeço em primeiro lugar a Deus como o arquiteto da minha vida; a minha família pela paciência, amor e apoio na distância, suas palavras sempre foram minha companhia; a minha amiga querida e os meus amigos que ainda continuam aconselhando sem importar a ausência. Também, ao meu orientador, o professor Douglas Eduardo Basso pela ajuda e guia no desenvolvimento do trabalho, assim como os meus colegas e todas as pessoas que fizeram parte desta etapa da minha vida contribuindo para a realização desta monografia.

Muita gente pequena, em lugares  
pequenos, fazendo coisas pequenas,  
podem mudar o mundo.

(GALEANO, Eduardo, 1974)

## RESUMO

ROMERO, Mario Lobo. **Implementação de um dispositivo portátil de roteamento para redes anônimas baseado em Raspberry Pi**. 2018. 49 p. Monografia de Especialização em Redes de Computadores e Teleinformática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

Neste trabalho se apresenta o processo para a Implementação e configuração de um dispositivo portátil, baseado no hardware da Raspberry Pi. O dispositivo, permite a navegação de um ou vários clientes através da rede TOR. O desenho da solução, fornece a capacidade de anonimização criando diferentes circuitos *onion* e roteando o tráfego dos clientes através deles, em um aparelho totalmente portátil. O resultado, é a localização anônima de cada cliente em um país diferenciado, embora todos estejam conectados à mesma rede local.

**Palavras-chave:** Rede TOR. Redes Anônimas. Segurança. Deep Web. Raspberry Pi.

## ABSTRACT

ROMERO, Mario Lobo. **Implementation of a portable routing device for anonymous networks based on Raspeberry Pi**. 2018. 49 p. Monografia de Especialização em Redes de Computadores e Teleinformática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

This paper presents the implementation and configuration process for a portable device based on Raspberry Pi hardware. This device allows navigation for one or more clients through the TOR network. The solution design provides the anonymity capability by creating different onion circuits and routing client traffic through them. It's results in the anonymous location of each client in a different country, all of them connected to the same local network.

**Keywords:** TOR Network. Anonymous Network. Security. Deep Web. Raspberry Pi.



## LISTA DE FIGURAS

Figura 1 - Tipos de redes na internet de acordo ao nível acesso.....	19
Figura 2 - Esquema circuito onion para serviço oculto.....	21
Figura 3 - Esquema circuito onion para Surface Web.....	22
Figura 4 - Autoridades de diretório.....	23
Figura 5 - Célula onion.....	24
Figura 6 - Esquema solução tipo Proxy Out.....	25
Figura 7 - Placa Raspberry Pi 3 Model B.....	27
Figura 8 - Descarga do Raspbian Linux.....	28
Figura 9 - Tela principal Etcher.....	28
Figura 10 - Caixa plástica de proteção.....	29
Figura 11 - Raspberry Pi com bateria portátil.....	30
Figura 12 - Estado serviço isc-dhcp-server.....	38
Figura 13 - Estado serviço hostapd.....	38
Figura 14 - Ponto de acesso habilitado.....	38
Figura 15 - Resposta NAT iptables.....	41
Figura 16 - Configuração hardware.....	41
Figura 17 - Prova conexão simultânea à rede TOR.....	43
Figura 18 - Prova conexão e localização rede TOR.....	44

## LISTA DE SIGLAS

AES	<i>Advance Encryption Standard</i>
ARPANET	<i>Advanced Research Projects Agency Network</i>
ARM	<i>Advance RISC Machine</i>
CCMP	<i>Counter Mode Cipher Block Chaining Message Authentication Code Protocol</i>
CPU	<i>Central Processing Unit</i>
CSI	<i>Camera Serial interface</i>
DARPA	<i>Defense Advanced Research Projects Agency</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
DNS	<i>Domain Name Service</i>
GPIO	<i>General Purpose Input-Output</i>
HDMI	<i>High Definition Multimedia Interface</i>
HTTP	<i>Hypertext Transfer Protocol</i>
IP	<i>Internet Protocol</i>
LAN	<i>Local Area Network</i>
MIT	<i>Massachusetts Institute of Technology</i>
NAT	<i>Network Address Translation</i>
PSK	<i>Pre-shared Key</i>
RAM	<i>Random Access Memory</i>
RISC	<i>Reduced instruction Set Computer</i>
SD	<i>Secure Digital</i>
SRI	<i>Stanford Research Institute</i>
SSH	<i>Secure SHell</i>
SSID	<i>Service Set Identifier</i>
TKIP	<i>Temporal Key Integrity Protocol</i>
TOR	<i>The Onion Router</i>
UC	<i>University of California</i>
UCLA	<i>University of California Los Angeles</i>
USB	<i>Universal Series Bus</i>
VPN	<i>Virtual Private Network</i>
WEP	<i>Wired Equivalent Privacy</i>

Wi-Fi	<i>Wireless Fidelity</i>
WPA	<i>Wi-Fi Protected Access</i>
WWW	<i>World Wide Web</i>

## SUMÁRIO

<b>1 INTRODUÇÃO .....</b>	<b>12</b>
1.1 CONSIDERAÇÕES INICIAIS .....	13
1.2 OBJETIVOS .....	14
1.2.1 Objetivo Geral .....	15
1.2.2 Objetivos Específicos .....	15
1.3 ESTRUTURA DO TRABALHO.....	15
<b>2 MARCO TEÓRICO .....</b>	<b>16</b>
2.1 INTRODUÇÃO ÀS REDES ANÔNIMAS .....	16
2.1.1 Internet Superficial (Surface Web) .....	17
2.1.2 Internet Profunda (Deep Web) .....	17
2.1.3 Internet Escura (Dark Web).....	18
2.2 A REDE TOR (THE ONION ROUTING).....	19
2.2.1 Nós (Relays).....	20
2.2.1.1 Nós de entrada (entry guard) .....	20
2.2.1.2 Nós de roteamento ou intermediários (relays).....	21
2.2.1.3 Nós de saída (exit relay).....	22
2.2.1.4 Autoridades de diretório .....	22
2.2.2 Circuitos .....	23
<b>3 INSTALAÇÃO E CONFIGURAÇÃO DO AMBIENTE .....</b>	<b>25</b>
3.1 RASPBERRY PI.....	26
3.1.1 Raspbian .....	27
3.1.1.1 Instalação de raspbian na raspberry Pi .....	27
3.1.2 Caixa Plástica de Proteção .....	29
3.1.3 Bateria Portátil .....	29
3.2 CONFIGURAÇÃO DO ROTEAMENTO.....	30
3.2.1 Servidor DHCP .....	30
3.2.2 Interfaces.....	33
3.2.3 Ponto de Acesso (Access Point) .....	34
3.2.4 Corta Fogo (Iptables).....	36
3.3 TOR.....	39
3.3.1 Corta Fogo para Tor (Iptables) .....	40
<b>4 CONSIDERAÇÕES FINAIS .....</b>	<b>42</b>
4.1 CONCLUSÕES .....	42
<b>REFERÊNCIAS.....</b>	<b>46</b>

## 1 INTRODUÇÃO

Para o correto entendimento das tecnologias que se descrevem neste documento, é importante analisar o processo da evolução da internet, assim como os principais acontecimentos que marcaram a transformação dramática da sociedade que desembocou no mundo digital atual.

A internet nasceu de uma ideia do psicólogo e cientista da computação Joseph Carl Robnett Licklider (LICKLIDER, 1960). Licklider desenvolveu a ideia da “Rede Galáctica” nos anos 60, como parte das pesquisas sobre relacionamento entre humanos e máquinas em quanto trabalhava como professor no MIT.

O conceito evoluiu através de alguns documentos onde se explicava a interação dos humanos e os computadores; primeiro a simbioses, no artigo *Man-Computer Symbiosis* (LICKLIDER, 1960); depois, *Online Man Computer and Communications* (LICKLIDER; CLARK, 1962) e finalmente, a introdução à ideia da rede galáctica desenvolvida com ajuda de Robert W. Taylor no artigo “*The Computers as a Communications Device*”, em 1968 (LICKLIDER; TAYLOR, 1968).

Para Licklider, a rede galáctica era “o meio principal e essencial de interação normativa para governos, instituições, corporações e indivíduos” (LICKLIDER; TAYLOR, 1968). Como pode-se observar, essa ideia é a essência da internet atual, a visão de Licklider transformou a humanidade.

Tempo depois, Licklider liderou DARPA e com ajuda dos trabalhos sobre transmissão de pacotes e redes de outros arquitetos da internet como Lawrence Roberts (ROBERTS, 1968), Robert Kahn e Vinton Cerf (KAHN; CERF, 1974) e muitos mais, construíram a infraestrutura física e lógica para a conexão dos 4 primeiros nós da ARPANET: UCLA, SRI, UC de Santa Bárbara e a Universidade de Utah. Assim, criou-se o primeiro antepassado da internet. A partir desse ponto, foram acrescentando-se o número de nós, aderindo computadores de universidades, centros de pesquisa, corpos militares, laboratórios, entre outros.

Como parte da necessidade de aproveitamento da rede, foi criado por parte de Ray Tomlinson, em 1971, um sistema de envio de mensagens misturando dos programas existentes na ARPANET: SNDMSG e CPYNET. Tomlinson, além, foi o inventor da @ para diferenciar o endereço do domínio e o nome do remetente e destinatário. Ele criou o que depois seria chamado correio eletrônico (TOMLINSON, 2018).

Em 1972, Robert Kahn introduziu o conceito que levou ao êxito rotundo da internet. Nesta definição, se permite a escalabilidade sem restrição nenhuma de topologia, infraestrutura ou distribuição dos nós, além disso, os protocolos principais não pertencem a nenhum proprietário e podem ser construídos pela comunidade. A internet foi concebida como uma “Rede Aberta”, ele chamou este conceito como “*Internetting*” (LAMBERT et al., 2005).

O ponto disruptivo na história da internet aconteceu em 1989 da mão do físico Tim Berners-Lee (BERNERS-LEE, 1989), arquiteto da WWW. A ideia de criar um protocolo como HTTP, que permitisse a interconexão de diferentes documentos da internet por meio de enlaces que pudessem ser indexados, revolucionou o jeito de entender e utilizar as redes, além, modelou a internet de hoje.

Com a chegada dos motores de pesquisa e a proliferação de computadores cada vez de menor tamanho e mais baratos, a internet desencadeou uma série de fenômenos sócias que transformaram a vida e a história do ser humano.

Depois dos motores de pesquisa, as redes sociais chegaram para mudar o paradigma do relacionamento das pessoas. Com o lançamento de “*The Facebook*” no 2004 (PHILLIPS, 2007) uma explosão de milhões de usuários começou a compartilhar suas vidas, interesses e tendências. A sociedade mudou para o ciberespaço.

As diferenças no modelo de indexação e busca de informação, assim como os métodos para permitir, ou não, a consulta dos dados, derivaram na criação de redes que procuram o anonimato das partes e a codificação do tráfego. Nos capítulos seguintes, serão expostas algumas tecnologias desenvolvidas para tal fim; se brindará uma pequena introdução ao porquê do uso do anonimato, e será comprovado um modelo econômico de implementação.

## 1.1 CONSIDERAÇÕES INICIAIS

Na era da conectividade, as redes sociais e a nuvem, a segurança tornou-se um valor e uma necessidade fundamental da sociedade. Os indivíduos levaram gradualmente suas vidas ao ciberespaço; desde as pequenas coisas até os processos sensíveis como suas finanças e seus dados mais privados.

Como parte desse processo de transformação digital, as nações e seus cidadãos transladaram também seus direitos e deveres para a nuvem. Este fato

fornece um novo estágio; por um lado, as pessoas têm responsabilidade do critério para compartilhar seus dados, mas ainda falta muita educação e consciência digital. Por outro, a regulação, normativa, controle e custódia dos dados são responsabilidade dos gigantes das telecomunicações e os governos.

Deste modo, em países com poucas liberdades e regímenes autoritários, esta situação é aproveitada para coar os direitos dos cidadãos.

O controle e censura sobre as comunicações e a informação, por parte dos governos autoritários, as empresas, ou grupos econômicos poderosos, diminui as possibilidades do livre pensamento dos cidadãos e perpetua as políticas de quem os oprime, além, dirige desde os comportamentos de consumo até a forma de pensar e agir politicamente a conveniência de quem tem o poder.

Como exemplo disso, durante o corrido do ano 2018 os dez países com maior quantidade de eventos de censura sobre os seus cidadãos são: Quirguistão, Mongólia, Turquia, Egito, Haiti, Guiana, Libéria, Ilha Reunião e Armênia (USERS, 2018). Pode se observar que a maioria de países do listado são muito pobres, e em constantes conflitos.

A possibilidade da anonimização se apresenta como uma oportunidade de evadir as restrições e permitir que nos países em conflitos bélicos ou sob regímenes com carência de respeito dos direitos humanos, periodistas e grupos de cidadãos possam mostrar ao mundo suas condições reais de vida. Além, consigam-se informar sobre os processos e oportunidades de apoio no mundo inteiro, isto, sem que sua vida ou bem-estar fossem expostos; fornecendo assim, uma esperança para estes povos.

Nessa perspectiva, é preciso proporcionar um jeito fácil e relativamente econômico para a instalação e configuração de um dispositivo que permita a navegação anônima por parte de um ou vários clientes, com total portabilidade e com independência do sistema que proveja saída à internet.

## 1.2 OBJETIVOS

Nesta seção são apresentados os objetivos geral e específicos do trabalho, relativos ao problema anteriormente apresentado.

### 1.2.1 Objetivo Geral

Descrever e explicar o processo de instalação e configuração de um dispositivo portátil de roteamento, para um ou vários clientes através da rede TOR baseado no hardware do *Raspberry Pi*.

### 1.2.2 Objetivos Específicos

Para atender ao objetivo geral neste trabalho de conclusão de curso os seguintes objetivos específicos serão abordados:

- Identificar a configuração ótima em termos de segurança e versatilidade para a instalação dos serviços de roteamento e anonimização no dispositivo *Raspberry Pi*.
- Comprovar a compatibilidade do hardware e as soluções a nível de software escolhidas para a solução do problema.
- Confirmar a correta anonimização do cliente utilizando ferramentas web.
- Evidenciar que, no evento da conexão simultânea de vários clientes, o dispositivo fornece um circuito *onion* e uma localização diferenciada para cada um dos participantes.

## 1.3 ESTRUTURA DO TRABALHO

Esta monografia de especialização, fornece uma solução baseada na união das experiências e trabalhos de vários pesquisadores e desenvolvedores no tema da anonimização, se procurou otimizar a relação custo-benefício pensando nas carências econômicas dos países alvo da solução.

Para facilitar o entendimento do leitor, esta monografia foi dividida em quatro seções. Na primeira, se realiza uma introdução e contextualização do problema e a possível solução. A seguir, na segunda seção, uma aproximação à fundamentação teórica da rede TOR e o hardware utilizado no desenvolvimento da solução. A terceira parte descreve o processo de instalação e configuração do dispositivo. Por último, as considerações finais e as conclusões obtidas no desenvolvimento da monografia.



## 2 MARCO TEÓRICO

### 2.1 INTRODUÇÃO ÀS REDES ANÔNIMAS

Na atualidade, cada vez se fala mais sobre as redes anônimas. O desconhecimento do funcionamento das tecnologias que conformam este tipo de redes, levaram à media e pessoas sem muitos conhecimentos técnicos, à difamação e tergiversação da informação ao redor delas. Isto, cria preconceitos sobre a sua utilização e impossibilita a exploração das oportunidades que fornecem os serviços de anonimização.

É importante anotar que, se bem muitas atividades dos criminosos têm cobertura sob o sigilo das redes anônimas, o crime existe como característica essencial do ser humano (FERNÁNDEZ, 2004), este tipo de redes se apresenta só como um meio que é destinado para tal fim. Sua utilização não constitui uma condição *sine qua non* do delito.

O crime na internet se remonta ao nascimento da rede de redes. A primeira transação de tráfico de drogas através da internet foi documentada no ano de 1972 e foi feita por estudantes do MIT e a Universidade de Stanford (FERNÁNDEZ, 2014) nessa data o fato aconteceu sob o domínio da legendaria ARPANET.

Para o correto entendimento do funcionamento das redes anônimas, é preciso conhecer a divisão da internet segundo os níveis de acesso à informação, assim como, entender a diferenciação de cada uma das camadas e a localização das redes anônimas neste esquema.

A internet está constituída por inúmeras redes interconectadas. Nestas redes, existem camadas lógicas de protocolos e tecnologias que permitem que algumas informações possam ser observadas de forma direta ou não. Segundo a possibilidade do acesso à informação, as camadas se classificam em ordem descendente; desde a mais superficial até a mais profunda (LAUTENSCHLAGER, 2016).

De acordo com o anterior, existem três tipos de redes: a) Internet Superficial (*Surface Web*), b) Internet Profunda (*Deep Web*), e c) Internet Escura (*Dark Web*).

### 2.1.1 Internet Superficial (Surface Web)

Se conhece como internet superficial, ao conjunto de sites, bancos de dados, serviços, aplicações, sistemas de mensageria e ecossistemas sociais indexados ou listados por os motores de pesquisa.

A acessibilidade aos dados neste tipo de redes não tem restrição nenhuma, qualquer pessoa com um motor de pesquisa pode visualizar o conteúdo da informação desta camada da internet.

Geralmente, os bancos de endereços eletrônicos dos motores de pesquisa são formados por robôs “*spider*” ou “*aranha*” que pesquisam de forma continua todos os sites da internet que não apresentem nenhuma restrição de acesso a seu conteúdo. Os resultados são indexados e listados para consulta dos clientes (GOOGLE, 2018).

Desde a criação da primeira proposta da *WWW* em 1989 (BERNERS-LEE, 1999) essa foi a intenção inicial da internet, interconectar por meio do protocolo *HTTP* infinidade de sites ao redor do mundo sem dificuldade. Embora, com o acréscimo sem controle do número de sites e de clientes, além do volcado excessivo de dados na internet, foi necessário começar a criar métodos para evitar o acesso a alguns tipos de informação. Assim, devagar, foi se construindo a era da segurança digital e a confidencialidade, dando passo à *Deep Web*.

### 2.1.2 Internet Profunda (Deep Web)

Aos poucos anos da criação da ARPANET, nos anos 70's, se começou a denominar internet escura ou profunda (não existiam diferencias pontuais ainda), aos sites que por motivos de segurança não eram listados ou indexados nos bancos de dados dos nodos da rede. Os engenheiros da ARPANET comentavam que eram sites dos que se tinha certeza da existência, mais permaneciam nas sombras, daí a denominação.

Se define como *Deep Web* ou Internet Profunda, a todo o conteúdo da internet: sites, bancos de dados, mensageria, sistemas de troca de arquivos, ecossistemas da nuvem, entre outros. Que por vontade própria ou por causa da aplicação de alguma tecnologia, não permitem a indexação ou listado dos seus conteúdos por parte dos motores de pesquisa. A *Deep Web* não é uma rede física separada, é uma camada

lógica formada por aplicações e protocolos de segurança e criptografia, que atua sobre as redes existentes (BIDDLE, 2018).

A Internet Profunda não necessariamente armazena informação confidencial ou criptografada. Existem numerosos bancos de dados acadêmicos, bibliotecas especializadas, artigos científicos, grupos de leitura, ativistas, ou simplesmente cidadãos que por uma, ou outra razão, preferem não compartilhar seus conteúdos com o mundo inteiro.

### 2.1.3 Internet Escura (Dark Web)

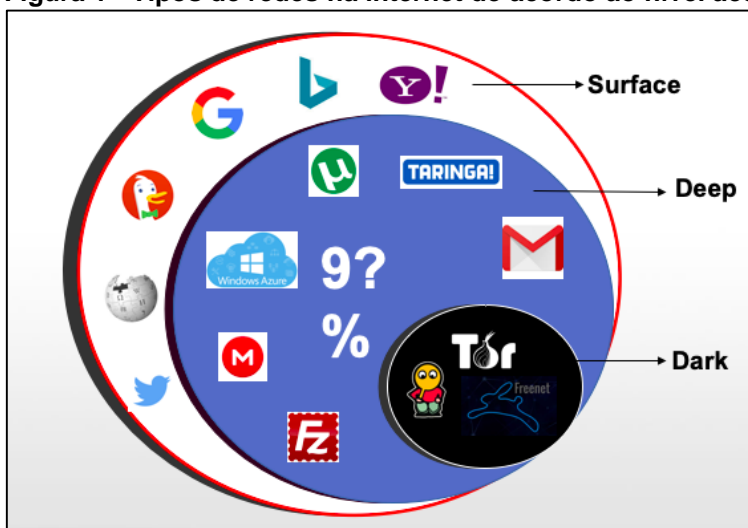
A mudança da sociedade para uma era digital, levou a internet para um processo de transformação, onde a confidencialidade ocupa cada vez mais um lugar relevante no desenvolvimento das tecnologias.

O fato da informação ser restrita nunca assegurou a confidencialidade ou o anonimato dos participantes numa comunicação. Governos de vários países censuram e monitoram as comunicações de seus cidadãos, corporações influenciam os hábitos de consumo e criminosos roubam os dados para seu lucro.

Estas preocupações, levaram a vários grupos de indivíduos desconformes com o *status quo*, à criação de tecnologias e protocolos que permitissem cobrir com uma ou varias camadas a informação, o jeito de transportá-la e manter sob anonimato as partes que a originam, assim nasceu a Internet Escura.

A Internet Escura ou *Dark Web* é parte da *Deep Web*, mas é considerada a camada mais profunda devido à criptografia aplicada. A *Dark Web* está formada pelas denominadas *DarkNets* ou Redes Escuras, que basicamente, são redes fechadas com acesso restrito e que precisam de aplicativos específicos para seu funcionamento. Se bem os conceitos de *DarkWeb* e *DarkNet* são muito próximos, é importante clarificar as diferenças, já que cada *DarkNet* contem protocolos e tecnologias específicas para sua utilização. Na Figura 1, pode-se observar a diferença das diferentes redes que compõem a internet e onde se concentra a maior parte da informação (ROMERO, 2018).

Figura 1 - Tipos de redes na internet de acordo ao nível acesso



Fonte: Romero (2018).

Em 1996 com o nascimento do conceito *The Onion Routing* (TOR) (GOLDSCHLAG; REED; SYVERSON, 1996) ou roteamento de cebola, se cria a oportunidade real de uma rede que cumpre os requisitos de anonimização, longe da censura e control dos governos e as corporações, a rede TOR.

Infelizmente nestes últimos anos, a notoriedade das *DarkNets* está direcionada ao uso de criminosos, deixando a um lado as vantagens das redes anônimas em sociedades carentes de direitos e liberdades, onde brinda oportunidades de comunicação.

## 2.2 A REDE TOR (THE ONION ROUTING)

A rede TOR (*The Onion Routing*) nasceu a partir dos estudos realizados no Laboratório de Pesquisa Naval dos Estados Unidos. A pesquisa desenvolvida por David M. Goldschlag, Michael G. Reed e Paul F. Syverson no ano 1996, descreve o método para anonimizar o tráfego de uma rede, utilizando o conceito de cobertura por camadas, como as de uma cebola, para ocultar a mensagem; sua origem e destino (GOLDSCHLAG; REED; SYVERSON, 1996).

A rede TOR é do tipo centralizada, quer dizer isto, que tem o foco do gerenciamento das tarefas e serviços em alguma entidade (PILIOURAS, 2004). Parece paradoxo que uma rede anônima possa focalizar em algum ponto esse labor, mas a rede TOR tem uma entidade distribuída de gerenciamento formada por vários nós que permitem uma infraestrutura mista, onde algumas características da rede

centralizada são alteradas para ser distribuídas, conseguindo assim, evadir as vulnerabilidades e o rastro da centralização.

Hoje, o projeto TOR, uma fundação sem ânimo de lucro é a encarregada da manutenção e desenvolvimento da rede e do software cliente para diferentes plataformas.

Os principais componentes da rede TOR são brevemente expostos na continuação.

### 2.2.1 Nós (Relays)

A tecnologia de roteamento de cebola (ou *Onion Routing*), está baseada no uso de nós distribuídos ao redor do mundo para formar circuitos virtuais. Existem diferentes tipos de nós de acordo ao serviço que fornecem à rede, estes, são formados por inúmeros voluntários anônimos esparzidos pelo globo, quantos mais nós compõem a rede, mais difícil é analisar o tráfego ou tentar identificar ou individualizar alguma conexão ou circuito (TOR, 2018a).

Os nós classificam-se de acordo a sua função em: *Proxy* de saída, *proxy* de entrada, e nós de roteamento ou *relays*. Um *proxy*, é um serviço, programa ou dispositivo que faz o trabalho de intermediário e controla de tráfego entre dois dispositivos (PILIOURAS, 2004).

A rede TOR é uma tecnologia muito versátil, que permite ao cliente a conexão de serviços *onion* ocultos na própria rede e serviços da internet superficial, agindo como VPN ou *proxy*. O aplicativo mais popular para a entrada a rede TOR é o *TOR Browser*, isto, já que a maior parte do tráfego que percorre a rede é HTTP. Porém, a rede permite a anonimização de qualquer tipo de serviço.

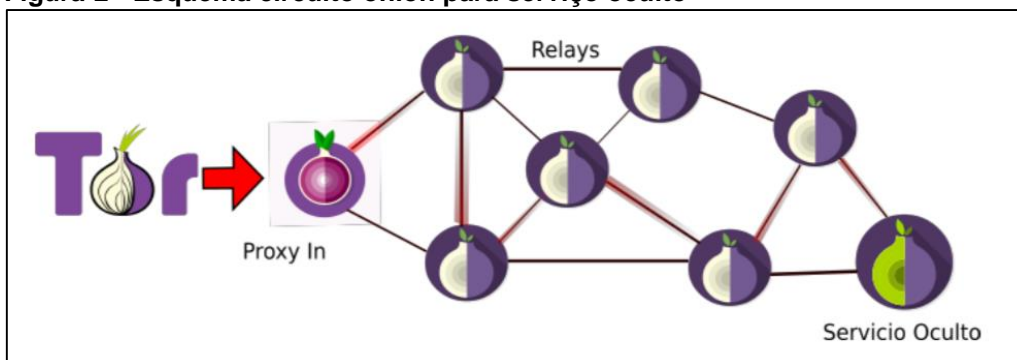
#### 2.2.1.1 Nós de entrada (entry guard)

O primeiro nó que usa o cliente para entrar na rede TOR é chamado nó de entrada. Independente do destino, serviço *onion* ou serviço da internet superficial, todos os clientes têm a obrigação de utilizar um *Entry Guard* cujo trabalho é levar as petições do cliente até a rede TOR.

Os serviços fornecidos só para o consumo dentro da rede TOR são chamados serviços *onion*. Em geral, os serviços fornecidos dentro das redes anônimas são chamados serviços ocultos ou *hidden services*. A Figura 2, apresenta o esquema para

acessar num serviço *onion* padrão, por meio de um circuito *onion* fornecido pela rede TOR (ROMERO, 2018).

**Figura 2 - Esquema circuito onion para serviço oculto**



Fonte: Romero (2018).

O nó de entrada tem uma tarefa de muita responsabilidade, já que é o único elemento da rede que conhece realmente o endereço IP do emissor, isto, o faz alvo de muitos ataques. As Autoridades de diretório são as únicas entidades que sabem com certeza quais nodos tem a bandeira *Entry guard*.

Na hora da entrada, o cliente faz uma solicitação para a rede, a qual é escutada pela Autoridade de diretório. Esta entidade descentralizada, escolhe um grupo de nós *Entry guard* aleatoriamente e entrega para o cliente quem realiza a escolha do nó para iniciar o circuito virtual. Uma vez é selecionado o nó de entrada, se prepara o circuito que vai utilizar na conexão.

O nó escolhido pelo cliente não muda com cada conexão, ele se mantém invariável um tempo estipulado pelo consenso da Autoridade, neste momento esse tempo é de 30 até 60 dias (TOR, 2018b).

#### 2.2.1.2 Nós de roteamento ou intermediários (relays)

Todos os nós que compõem o circuito virtual localizados entre o nó de entrada e o nó de saída, ou, o nó de entrada e um serviço *onion*, são chamados nós de roteamento.

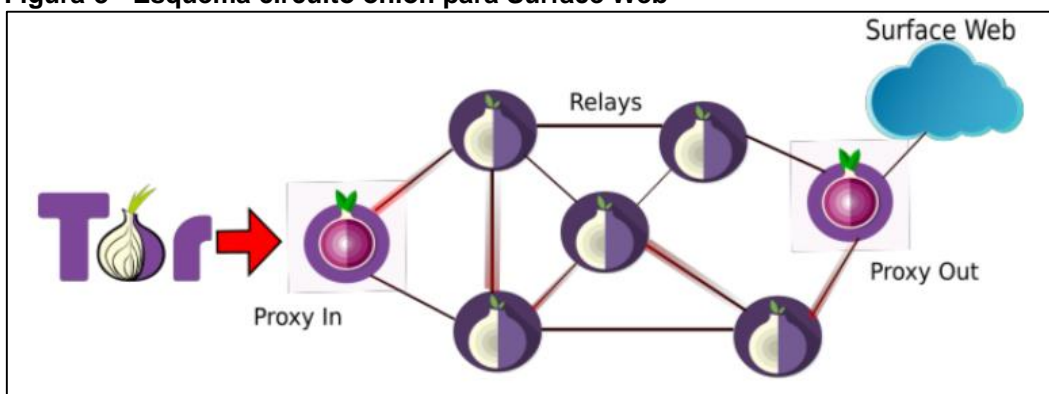
O êxito da rede TOR depende em maior parte da existência desses nós, já que quantos mais nós constroem o circuito, mais difícil é tentar fazer o seguimento de uma comunicação. Um circuito virtual tem como mínimo 3 nós intermediários e máximo o protocolo se encontra parametrizado com 6 saltos (TOR, 2018b), é possível acrescentar este número, mas a eficiência da rede sofre uma queda significativa.

### 2.2.1.3 Nós de saída (exit relay)

Como se falou no apartado anterior, a rede TOR tem a possibilidade de acesso aos serviços *onion*, mas também, tem a possibilidade de acesso à *Surface Web* agindo como passarela ou *proxy out*. O nó de saída é aquele que fornece a saída à Internet Superficial.

Do mesmo modo que o nó de entrada, o nó de saída carrega a responsabilidade de ser o único elemento da rede que conhece a IP do serviço final acessado pelo cliente. Na Figura 3, pode-se observar o esquema padrão de um circuito *onion* preparado para a navegação na internet superficial, neste modelo, a IP que o serviço superficial consegue detectar é aquela fornecida pelo ultimo nó, no lugar do mundo onde ele se localize (ROMERO, 2018).

**Figura 3 - Esquema circuito onion para Surface Web**



Fonte: Romero (2018).

De fato, a rede TOR não fornece segurança, apenas anonimato, por isso, é altamente recomendado que as comunicações e o acesso aos serviços sejam feitos com camadas de criptografia intrínsecas ao próprio serviço e não dependa da rede TOR para essa tarefa.

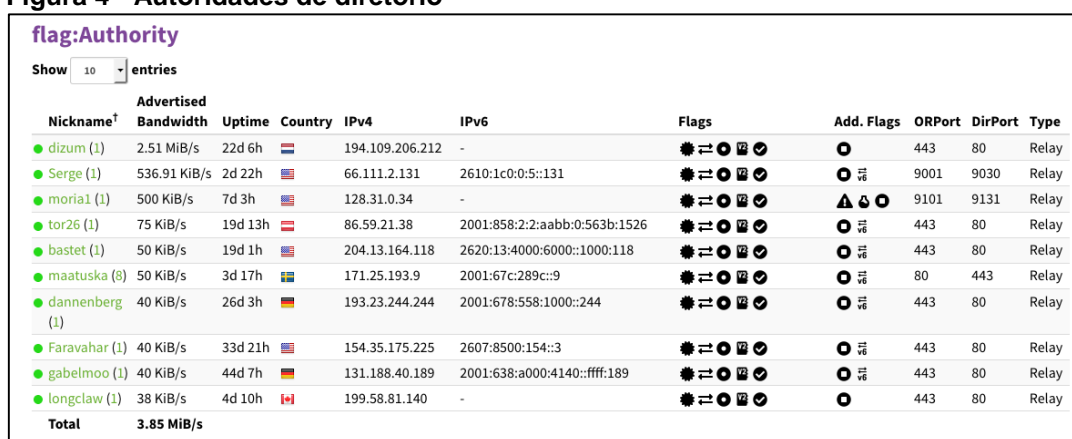
### 2.2.1.4 Autoridades de diretório

A rede TOR é definida como centralizada graças às Autoridades de diretório. Estas autoridades, são nós especiais os quais contem listados dos nós da rede; efetuam uma revisão geral e geram um consenso sobre a função e a participação deles na rede, que posteriormente, é replicado aos clientes.

Apesar de eles centralizarem e focalizarem o gerenciamento, o jeito de fazê-lo distribuindo a responsabilidade em vários nós espalhados, faz que as vulnerabilidades sejam diminuídas e o rastro anulado.

Por defeito, o *Tor Browser* tem armazenado o listado das Autoridades de diretório, isto, para prevenir que sejam substituídas e utilizadas para extrair informação do comportamento da rede. Na atualidade existem 10 Autoridades de diretório, elas podem ser consultadas no site oficial do projeto TOR (TOR, 2018c). Na Figura 4, são apresentadas as autoridades disponíveis à data de realização desta monografia.

**Figura 4 - Autoridades de diretório**



Nickname†	Advertised Bandwidth	Uptime	Country	IPv4	IPv6	Flags	Add. Flags	ORPort	DirPort	Type
● <a href="#">dizum</a> (1)	2.51 MiB/s	22d 6h		194.109.206.212	-			443	80	Relay
● <a href="#">Serge</a> (1)	536.91 KiB/s	2d 22h		66.111.2.131	2610:1c0:0:5::131			9001	9030	Relay
● <a href="#">moria1</a> (1)	500 KiB/s	7d 3h		128.31.0.34	-			9101	9131	Relay
● <a href="#">tor26</a> (1)	75 KiB/s	19d 13h		86.59.21.38	2001:858:2:2:aabb:0:563b:1526			443	80	Relay
● <a href="#">bastet</a> (1)	50 KiB/s	19d 1h		204.13.164.118	2620:13:4000:6000::1000:118			443	80	Relay
● <a href="#">maatuska</a> (8)	50 KiB/s	3d 17h		171.25.193.9	2001:67c:289c::9			80	443	Relay
● <a href="#">dannenberg</a> (1)	40 KiB/s	26d 3h		193.23.244.244	2001:678:558:1000::244			443	80	Relay
● <a href="#">Faravahar</a> (1)	40 KiB/s	33d 21h		154.35.175.225	2607:8500:154::3			443	80	Relay
● <a href="#">gabelmoo</a> (1)	40 KiB/s	44d 7h		131.188.40.189	2001:638:a000:4140::ffff:189			443	80	Relay
● <a href="#">longclaw</a> (1)	38 KiB/s	4d 10h		199.58.81.140	-			443	80	Relay
<b>Total</b>	<b>3.85 MiB/s</b>									

Fonte: Tor (2018c).

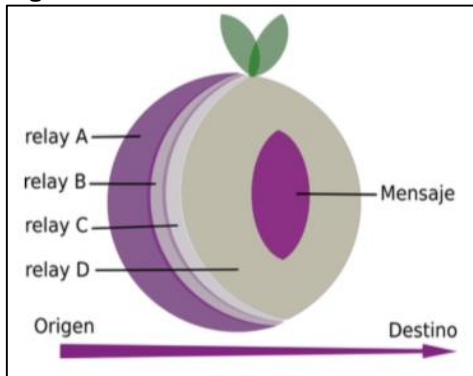
O protocolo das Autoridades de diretório, utiliza medições e algoritmos de validação para votação coletiva, o que faz que a rede acrescente sua eficiência liberando os nós de descarregar os descritores inteiros, logo, só certas bandeiras são atualizadas nos clientes.

## 2.2.2 Circuitos

O protocolo *onion* foi chamado assim devido à analogia com as camadas de uma cebola. O processo de criptografado e empacotado da mensagem é feito camada a camada cada vez que ela passa por um nó, ficando em uma espécie de envoltório dentro de outro envoltório adicionado por cada nó participante no circuito.

As camadas de criptografia são adicionadas de forma incremental por meio de chaves TLS efêmeras. Na Figura 5, é possível observar uma analogia, onde se descreve o processo de criptografado da informação (ROMERO, 2018).



**Figura 5 - Célula onion**

Fonte: Romero (2018).

Antes do seu envio, ainda na Figura 5, a informação é criptografada com as chaves do nó “D”, depois já na formação do circuito com as chaves do nó “C”, depois do “B” e por último o nó “A”, criando um pacote de cifrado sobre cifrado com tantas camadas quanto número de nós existam no circuito virtual.

O processo contrário é feito para o descifrado da mensagem, camada por camada até chegar ao centro da célula, onde se encontra a informação enviada pelo emissor.

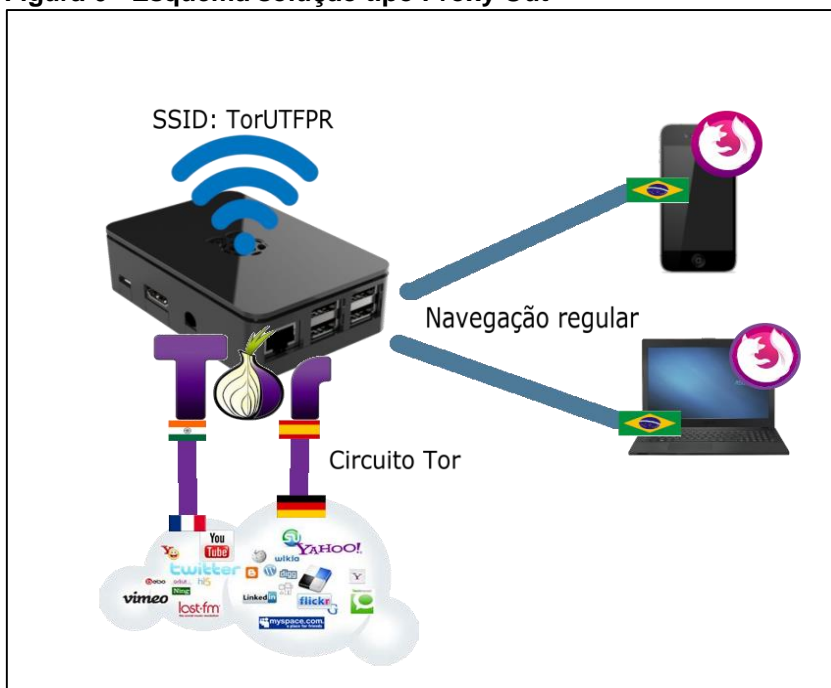
### 3 INSTALAÇÃO E CONFIGURAÇÃO DO AMBIENTE

Neste capítulo, serão apresentados o processo e as ferramentas necessárias para a instalação e configuração da solução de anonimização de que trata este documento.

Muitas das configurações aqui apresentadas são obra de diversos pesquisadores da *Deep Web*, neste documento se procurou juntar e ordenar, depois de múltiplas provas, as melhores e mais concisas delas para conseguir articular um desenho fiável e seguro que forneça uma alta portabilidade, além disso, se buscou uma baixa inversão em termos econômicos e uma robustez que permita o trabalho em ambientes complexos.

Na Figura 6, é apresentado um esquema da solução, onde pode-se observar que para cada cliente conectado na *Raspberry* é criado um circuito que fornece uma localização diferente para os sistemas de detecção nos serviços da *Surface Web*. Além disso, mostra como não é preciso um navegador especial tipo *Tor Browser* para conseguir acesso anônimo, isso, graças a que a solução fornece um circuito particular para cada cliente sem importar a plataforma ou navegador utilizado. É importante notar que só no caso de requerer acessar num serviço oculto *.onion* deveria utilizar-se o navegador *TorBrowser*.

Figura 6 - Esquema solução tipo Proxy Out



Fonte: Autoria própria.

### 3.1 RASPBERRY PI

Um dos pontos angulares da solução fornecida neste documento, é a possibilidade da configuração num hardware relativamente econômico e com alta portabilidade.

Das opções do mercado, a *Raspberry Pi* provê um desenho com alto rendimento num preço relativamente baixo (R\$ 200,00)<sup>1</sup>, as especificações apresentadas neste modelo B BCM2837 - MPU ARM Cortex-A53 são listadas na sequência (RASPBERRY, 2018a):

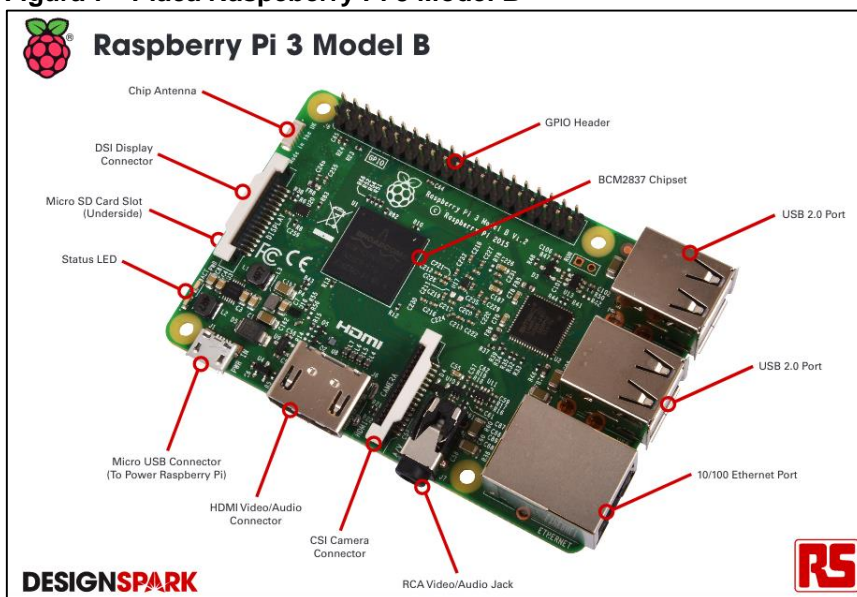
- Processador: Quad Core 1.2GHz Broadcom BCM2837 64bit CPU
- Memória: 1 Gb RAM
- Wifi: BCM43438 *wireless* LAN e *Bluetooth Low Energy* (BLE)
- Rede: 100 Base *Ethernet*
- Conexão: 40-pin *extended* GPIO
- USB: 4 USB 2 ports
- Áudio: 4 *Pole stereo* e porta de vídeo composto
- Vídeo: *Full size HDMI*
- Câmera: CSI *câmera port*
- Tela: *DSI display port*
- Armazenamento: MicroSD
- Energia: *Micro* USB 2.5<sup>a</sup>

Segundo os criadores, a *Raspberry Pi* é definida como uma placa de computador compacta que fornece, devido a seu preço e configuração, um sem-fim de possibilidades sem as restrições econômicas típicas das novas tecnologias. Na Figura 7, é apresentada a placa e seus componentes principais.

---

<sup>1</sup> Consulta disponível em: <[https://www.amazon.com.br/Placa-Raspberry-Quadcore-1-2ghz;Bluetooth/dp/B01CD5VC92/ref=sr\\_1\\_1?ie=UTF8&qid=1541376548&sr=8-1&keywords=raspberry](https://www.amazon.com.br/Placa-Raspberry-Quadcore-1-2ghz;Bluetooth/dp/B01CD5VC92/ref=sr_1_1?ie=UTF8&qid=1541376548&sr=8-1&keywords=raspberry)>. Acesso em: 18 out. 2018.

Figura 7 - Placa Raspberry Pi 3 Model B



Fonte: Raspberry (2018a).

### 3.1.1 Raspbian

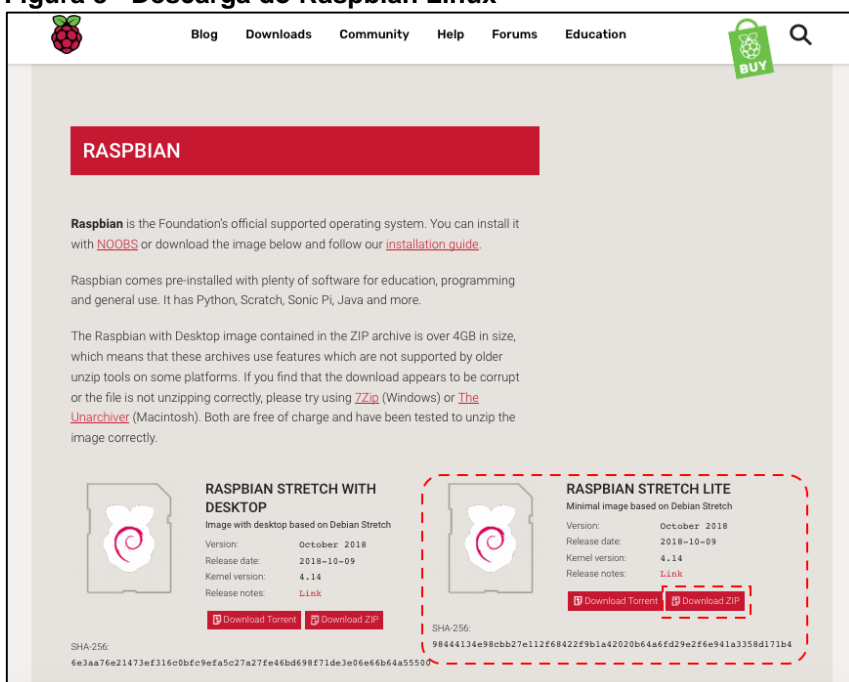
Segundo seus desenvolvedores, *Raspbian* é um sistema operativo de código aberto baseado na distribuição *Linux Debian*, otimizado para o hardware da *Raspberry Pi* sobre plataforma com processador ARM (RASPBIAN, 2018).

#### 3.1.1.1 Instalação de raspbian na raspberry Pi

O primeiro passo para conseguir embarcar a solução de anonimização, é contar com um sistema operativo para controlar o hardware da *Raspberry Pi*. A seguir, se explicam os passos para a instalação da distribuição *Linux Raspbian*:

- Descarregar a imagem do sistema operacional localizada no site oficial de *Raspberry* (Figura 8), no endereço disponível em: <https://www.raspberrypi.org/downloads/raspbian/>, acesso em: 18 out. 2018. Selecionar a opção *Raspbian Scretch lite* sem entorno gráfico, já que para a versão servidor não é preciso, além disso, são economizados recursos de hardware.

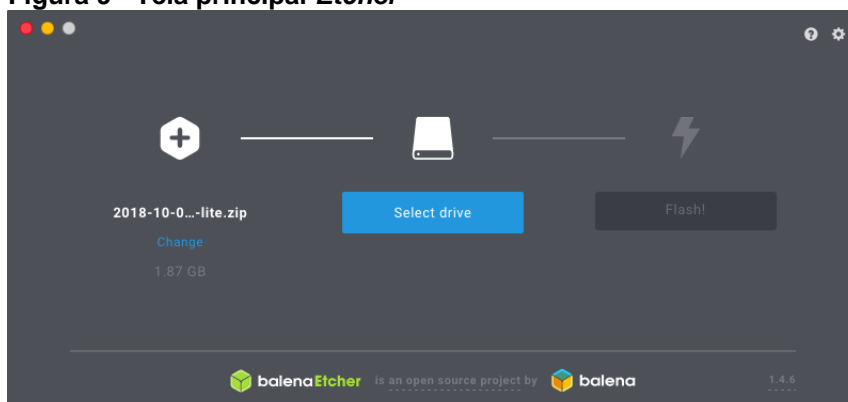
**Figura 8 - Descarga do Raspbian Linux**



Fonte: Raspbian (2018).

- b) Uma vez descarregada a imagem em formato zip, é necessário gravar o sistema operativo no cartão *MicroSD*. Para isso, é recomendado o uso do programa *Etcher*, disponível para as plataformas *Windows*, *Linux* e *MacOs* no seguinte endereço disponível em: <<https://www.balena.io/etcher/>>, acesso em: 18 out. 2018. Escolhe-se o arquivo “.zip” da distribuição *Raspbian* sem descompactar; se seleciona o cartão *MicroSD* e por último, com o botão flash, procede-se a gravação da imagem na unidade correspondente (Figura 9).

**Figura 9 - Tela principal *Etcher***



Fonte: Autoria própria.

- c) A continuação, a *MicroSD* é colocada na *Raspberry Pi*. Uma vez ligada a Raspberry, a sequência de iniciação leva à tela de autenticação; as credenciais padrão são: usuário: “*pi*”, senha: “*raspberry*”.

d) Finalmente, antes de começar a configuração dos pacotes de roteamento é preciso obter a última versão dos repositórios e do software instalado. Para isso, são usados os comandos: *apt-get update*, *apt-get upgrade*.

### 3.1.2 Caixa Plástica de Proteção

Para evitar que a placa seja danificada por alguma condição ambiental ou contaminação elétrica, é acondicionada uma caixa plástica de proteção que permite a conexão de qualquer periférico, sem problemas.

Como pode-se observar na Figura 10, além do case ou caixa protetora é adicionado um dissipador localizado sobre o chip de comunicação *Wifi* que permite um trabalho mais forte e prolongado.

**Figura 10 - Caixa plástica de proteção**



**Fonte: Autoria própria.**

### 3.1.3 Bateria Portátil

Caso de não se encontrar próximo a uma fonte de eletricidade, para conseguir independência e portabilidade, é preciso fornecer a solução de energia suficiente por meio de uma bateria de pelo menos 5 volts e 2 amperes.

De acordo a quantidade de células da bateria, ela terá um maior ou menor tempo de independência, mas isso é diretamente proporcional ao tamanho. Na Figura 11, pode-se constatar o tamanho de uma bateria que pode fornecer aproximadamente uma hora de independência ao sistema.

Figura 11 - *Raspberry Pi* com bateria portátil



Fonte: Autoria própria.

## 3.2 CONFIGURAÇÃO DO ROTEAMENTO

O esquema de roteamento para a solução, precisa da configuração de vários serviços que permitem o encaminhamento dos pacotes transmitidos entre a rede privada usada pelos clientes e a rede TOR.

O primeiro passo, é realizar a configuração do servidor que aloca automaticamente os endereços IP na rede privada, o servidor DHCP. Depois, é preciso realizar a configuração das interfaces utilizadas para a conexão tanto dos clientes na rede privada, quanto do dispositivo que fornece acesso à internet. Por último, se devem configurar as tabelas de roteamento para redirecionar os pacotes desde a rede privada até o primeiro nó do circuito virtual *onion*, igual no sentido contrario.

A continuação é explicado o processo da instalação e configuração dos serviços antes mencionados, tendo como guia a documentação provida pela casa criadora do hardware Raspberry Pi (RASPBERRY, 2018b).

### 3.2.1 Servidor DHCP

Um servidor DHCP ou de protocolo de configuração dinâmica de *host*, permite a alocação dinâmica dos endereços IP, além de outras configurações de rede em cada

cliente, que facilitam a conexão e a comunicação com outras redes. O serviço DHCP também possibilita a alocação estática de endereços (Forouzan, 2010).

Para o correto funcionamento do sistema de alocação de endereços IP, deve-se instalar e configurar em primeiro lugar o serviço *hostapd* (*host access point daemon*), este serviço permite que o dispositivo possa-se comportar como um ponto de acesso (*Access Point*) e consiga autenticar clientes na sua rede.

O segundo serviço a instalar, trata-se do servidor de alocação de endereços IP *isc dhcp server* fornecido nas distribuições *Debian*.

A instalação dos serviços é realizada por meio do comando:

```
$ sudo apt-get install hostapd isc-dhcp-server
```

Logo da instalação do servidor DHCP e o *hostapd*, é indispensável a instalação do firewall dos sistemas Linux conhecido como *iptables*, o nome real do software é *Netfilter*. *Netfilter* se apresenta como uma suíte muito completa de ferramentas de filtrado e direcionamento de pacotes que trabalha no nível do *kernel* do Linux da qual *iptables* é uma parte muito estável e confiável (NETFILTER, 2018).

A instalação de *iptables* é realizada com o seguinte comando:

```
$ sudo apt-get install iptables-persistent
```

Uma vez instalados os serviços, se realiza a configuração do serviço DHCP. Para o exemplo é utilizado o editor de texto *nano*, mas o arquivo de configuração pode ser modificado com o editor de preferência do leitor. Para isso, é utilizado o comando:

```
$ sudo nano /etc/dhcp/dhcpd.conf
```

O arquivo *dhcpd.conf* contém um *template* com muitas linhas guia, que para o caso da implementação atual não são necessárias. Devido a isso, tem a possibilidade de deixar as linhas guia e comentar ou adicionar as que são precisas para a configuração. No arquivo devem ser comentadas as linhas que correspondem ao nome de domínio de exemplo e os servidores do sistema de domínio DNS. Para comentar é preciso adicionar o símbolo “#” ao começo da linha.

```
#option domain-name "example.org";  
#option domain-name-servers ns1.example.org, ns2.example.org;
```

Caso se escolha deixar só as linhas que serão utilizadas na configuração DHCP, o arquivo ficaria assim:



Os parâmetros de configuração são listados a continuação:

```
1. default-lease-time 600;
2. max-lease-time 7200;
3. ddns-update-style none;
4. authoritative;
5. subnet 192.168.100.0 netmask 255.255.255.0 {
6.     range 192.168.100.10 192.168.100.50;
7.     option broadcast-address 192.168.100.255;
8.     option routers 192.168.100.1;
9.     default-lease-time 600;
10.    max-lease-time 7200;
11.    option domain-name "local";
12.    option domain-name-servers 1.1.1.1, 1.0.0.1;
13. }
```

Na linha 1, o *default-lease-time* é utilizado para indicar o tempo de concessão de um endereço IP caso o cliente não indique ele manualmente, o tempo é apresentado em segundos (GÓMEZ, 2013).

O parâmetro *max-lease-time* da linha 4, indica o tempo em segundos da concessão de um endereço IP caso o cliente configure um tempo maior ao *default-lease-time*, este tempo também é apresentado em segundos.

A linha 5, contém o parâmetro *ddns-update-style* que é utilizado para indicar se o servidor DHCP fará atualizações do nome do cliente baseado no serviço DNS, neste caso, o servidor DNS não é utilizado na rede local, portanto, o valor é *none* (GÓMEZ, 2013).

A linha 6, *authoritative* é muito importante para a segurança do servidor, este parâmetro permite que o servidor consiga responder uma mensagem DNSNACK de denegação, ante algum requerimento de um endereço IP não válido. O parâmetro *authoritative*, além disso, *adiciona* cifrado ao diálogo entre cliente e servidor; fornecendo uma capa de segurança contra possíveis atacantes (GÓMEZ, 2013).

As linhas seguintes, servem para configurar os parâmetros da rede: uma sub rede 192.168.100.0 com máscara 255.255.255.0; o rango de endereços para alocar entre 192.168.100.10 e 192.168.100.50 o que resulta em 40 clientes; configuração do endereço de difusão ou *broadcast* 192.168.100.255 e o *gateway* ou porta de enlace de roteamento 192.168.100.1.

Além das configurações básicas da rede, também é possível configurar o endereço do sistema de resolução de nomes, que para este caso, utiliza os DNS da

*OpenDNS*<sup>2</sup> 1.1.1.1 e 1.0.0.1. As razões para a escolha destes servidores são, entre outros, sua velocidade e independência. Como a rede local não pertence a nenhum servidor de domínio, se configura o parâmetro “*local*”.

O seguinte passo na configuração do serviço é escolher a interface de rede que servirá como ponto de acesso. Com o comando “*ifconfig*” pode-se observar o nome da interface sem fios; para este caso “*wlan0*”. Segundo isso, se deve modificar o arquivo *isc-dhcp-server* para adicionar essa interface:

```
$ sudo nano /etc/default/isc-dhcp-server
```

Se deve procurar a linha como o parâmetro *INTERFACESV4* e modificar, assim:

```
INTERFACESv4="wlan0"
```

### 3.2.2 Interfaces

Seguidamente à configuração do serviço DHCP, é preciso configurar o arquivo “*interfaces*”, para indicar o comportamento das portas na hora da conexão de algum dispositivo à *Raspberry*, além, habilitar o serviço DHCP com perfil de servidor na interface sem fios. É importante realizar a configuração como perfil de cliente nas outras interfaces, para quando seja preciso obter um endereço de outra rede, como a internet, por exemplo. Para a modificação do arquivo é utilizado o comando:

```
$ sudo nano /etc/network/interfaces
```

Este arquivo contém todas as informações acerca do comportamento das interfaces na hora de uma conexão.

A primeira interface listada é “*lo*” ou *loopback*, é uma interface virtual local utilizada para vários métodos de roteamento de pacotes do sistema operativo, também para identificar e dirigir o tráfego dentro do sistema (JUNIPER, 2018).

Todas as linhas que começam com “*auto*” serão detectadas e carregadas automaticamente no arranque do sistema. Para definir uma interface lógica é preciso incluir o termo “*iface*” no início da linha, depois, o nome da interface, e para habilitar o protocolo TCP/IP se deve adicionar o termo “*inet*” (DEBIAN, 2018). As linhas a adicionar são:

---

<sup>2</sup> Página oficial da OpenDNS. Disponível em: <<https://www.opendns.org>>. Acesso em: 17 out. 2018.

```
auto lo
iface lo inet loopback
```

Do mesmo modo, é adicionada a interface *Ethernet*. O termo “*allow-hotplug*” é utilizado para indicar que ao momento de conectar um dispositivo nesta interface possa ser detectado bem ao início do sistema, caso estar presente, ou depois em qualquer momento que suceda a conexão. Além da detecção, depois do “*inet*” é adicionado o parâmetro “*dhcp*” que habilita o serviço nesta interface (DEBIAN, 2018).

```
auto eth0
allow-hotplug eth0
iface eth0 inet dhcp
```

A interface seguinte é a USB, isto, caso ocorra uma conexão por meio de um aparelho celular ou modem 4G, fato muito comum quando se fala de um aparelho que fornece portabilidade.

```
auto usb0
allow-hotplug usb0
iface usb0 inet dhcp
```

Finalmente, é configurada a interface sem fios *wlan0*, é aproveitada a configuração para indicar o endereço IP estático 192.168.100.1 e a máscara da rede, isso, já que essa interface atua como o servidor DHCP local.

```
auto wlan0
allow-hotplug wlan0
iface wlan0 inet static
address 192.168.100.1
netmask 255.255.255.0
```

### 3.2.3 Ponto de Acesso (Access Point)

A configuração do ponto de acesso é indispensável para o êxito da solução proporcionada, repare-se que é a rede que os clientes utilizarão como porta de entrada que os interconectará com a rede TOR.

O arquivo de configuração do ponto de acesso é o relativo ao serviço *hostapd*.

Os parâmetros de configuração são listados a continuação:

```
1. interface=wlan0
2. ssid=TorUTFPR
3. country_code=BR
4. hw_mode=g
5. channel=6
6. macaddr_acl=0
7. auth_algs=1
8. ignore_broadcast_ssid=0
9. wpa=2
10. wpa_passphrase=TorUTFPR
11. wpa_key_mgmt=WPA-PSK
12. wpa_pairwise=CCMP
13. wpa_group_rekey=86400
14. ieee80211n=1
15. wme_enabled=1
```

Os parâmetros de configuração são explicados na sua ordem a seguir, de acordo à documentação provida pelo criador (MALINEN, 2016):

- *interface*: A interface destinada para servir de ponto de acesso, *wlan0*.
- *ssid*: O identificador da rede, consta de um máximo de 32 caracteres alfanuméricos, neste caso foi chamada TorUTFPR.
- *country\_code*: Código do país, para o caso seria Brasil ou BR.
- *hw\_mode*: Corresponde à tecnologia do hardware Wi-Fi, tecnologia 802.11 g que está sobre os 2.4 GHz é utilizada com este modelo da Raspberry.
- *channel*: O canal escolhido para o trabalho, pode depender da interferência de outros dispositivos WiFi. O canal 6 foi utilizado nesta solução.
- *macaddr\_acl*: Este parâmetro é ativado caso se precise o controle do acesso por meio da MAC dos dispositivos clientes, o valor 0 indica que não é habilitada essa característica.
- *auth\_algs*: O algoritmo de autenticação é configurado de acordo aos parâmetros: 1=WPA, 2=WEP, 3=Both. É escolhido o algoritmo WPA.
- *wpa*: É selecionado o sistema de criptografado que provê a segurança na autenticação da conexão, para a solução é escolhida a versão 2 do wpa.
- *wpa\_passphrase*: Neste parâmetro se configura a senha da conexão Wi-Fi, TorUTFPR.
- *wpa\_key\_mgmt*: A administração da senha WPA é feita por meio de WPA-PSK com chave compartilhada.

- *wpa\_pairwise*: É escolhido o protocolo de criptografado CCMP com AES para tecnologias WPA, que é o substituto do vulnerável TKIP.
- *wpa\_group\_rekey*: Intervalo expressado em segundos para requerer de novo a chave de autenticação da rede durante o dia. O tempo padrão está em 86400 segundos.
- *ieee80211n*: É habilitada a tecnologia 802.11n.
- *wme\_enabled*: Fornece prioridades aos pacotes que são trafegados pela rede, a opção 1 não apresenta nenhuma prioridade. Caso o vídeo ou a voz sejam prioridade devem-se escolher as opções 4 e 7 respectivamente.

Para conseguir que o serviço seja executado de acordo à configuração apresentada, é preciso incluí-lo no arquivo do demônio de Linux localizado na rota */etc/default/hostapd*, o comando para realizar esta operação é:

```
$ sudo nano /etc/default/hostapd
```

Uma vez aberto o arquivo, se deve procurar a linha *#DAEMON\_CONF=""* para tirar o comentário e adicionar a rota do arquivo de configuração do *hostapd*, a linha deveria ficar do seguinte modo:

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

Do mesmo modo, é realizada essa operação no arquivo do início do sistema *init.d*, se realiza a edição assim:

```
$ sudo nano /etc/init.d/hostapd
```

Se procura a linha que contem *#DAEMON\_CONF=""*, e é substituída por:

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

### 3.2.4 Corta Fogo (Iptables)

A configuração mais importante para conseguir que o dispositivo reencaminhe pacotes, permitindo o tráfego entre a rede local e a rede TOR, é habilitar o parâmetro *ip\_forward*. Para isso, se deve modificar o arquivo *sysctl.conf* por meio do seguinte comando:

```
$ sudo nano /etc/sysctl.conf
```

Em seguida é preciso modificar e apagar o símbolo “#” na linha que contem o parâmetro *ip\_forward*.

```
net.ipv4.ip_forward=1
```

Do mesmo modo, se deve habilitar o encaminhamento de pacotes IPV4 no *kernel* do sistema imediato, executando o comando:

```
$ sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"
```

A continuação, são adicionadas as linhas de *iptables* que permitem o encaminhamento dos pacotes.

```
1. $ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
2. $ sudo iptables -A FORWARD -i eth0 -o wlan0 -m state --state
   RELATED,ESTABLISHED -j ACCEPT
3. $ sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
```

Segundo a documentação provida para *iptables* (RHEL, 2005), a linha 1, é utilizada para modificar a tabela NAT adicionando o argumento POSTROUTING o qual indica que os pacotes se devem encaminhar pela interface “*eth0*” e fazer mascaramento na interface

Na linha 2, se indica que os pacotes que entrarem pela interface “*eth0*” serão encaminhados pela interface *wlan0*, além, é ativado o módulo *state* para indicar que os pacotes que coincidam com os estados de conexão *RELATED* ou *ESTABLISHED* possam ser aceitos.

A linha 3, contem as instruções para que todos os pacotes que entrarem pela interface *wlan0* possam ser encaminhados até interface *eth0*.

Por último, tem que ser salvas as modificações nas tabelas de roteamento, para isso é usado o comando:

```
$ sudo sh -c "iptables-save > /etc/iptables/rules.v4"
```

Além disso, é ativado o ponto de acesso por meio do comando:

```
$ sudo /usr/sbin/hostapd /etc/hostapd/hostapd.conf
```

Finalmente, é necessário o reinício dos serviços DHCP e *hostapd*, executando os seguintes comandos:

```
$ sudo service hostapd start
$ sudo service isc-dhcp-server start
$ sudo update-rc.d hostapd enable
$ sudo update-rc.d isc-dhcp-server enable
```

Neste ponto, a rede sem fios deve estar disponível com o nome TorUTFPR e ser funcional para o acesso e autenticação, mas ainda sem conexão à rede TOR.

Pode-se comprovar o estado dos serviços instalados e configurados, assim:

```
$ sudo service isc-dhcp-server status
$ sudo service hostapd status
```

Nas Figuras 12 (Estado serviço isc-dhcp-server) e 13 (Estado serviço hostapd), pode-se observar estado dos serviços.

**Figura 12 - Estado serviço isc-dhcp-server**

```
pi@raspberrypi:~$ sudo service isc-dhcp-server status
isc-dhcp-server.service - LSB: DHCP server
Loaded: loaded (/etc/init.d/isc-dhcp-server; generated; vendor preset: enable)
Active: active (running) since Sat 2018-06-30 17:18:08 -03; 10h ago
Docs: man:systemd-sysv-generator(8)
Process: 625 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=
CGroup: /system.slice/isc-dhcp-server.service
└─664 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf wlan0
```

Fonte: Autoria própria.

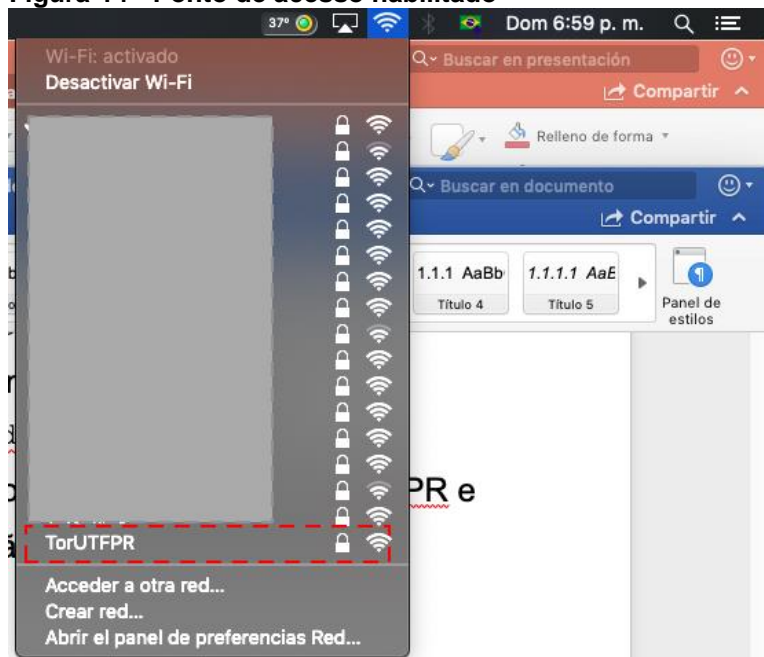
**Figura 13 - Estado serviço hostapd**

```
pi@raspberrypi:~$ sudo service hostapd status
hostapd.service - LSB: Advanced IEEE 802.11 management daemon
Loaded: loaded (/etc/init.d/hostapd; generated; vendor preset: enabled)
Active: active (running) since Sat 2018-06-30 17:18:05 -03; 10h ago
Docs: man:systemd-sysv-generator(8)
Process: 626 ExecStart=/etc/init.d/hostapd start (code=exited, status=0/SUCCESS)
CGroup: /system.slice/hostapd.service
└─655 /usr/sbin/hostapd -B -P /run/hostapd.pid /etc/hostapd/hostapd.c
```

Fonte: Autoria própria.

Na Figura 14, pode-se observar que o ponto de acesso se encontra disponível, embora sem conexão à rede TOR.

**Figura 14 - Ponto de acesso habilitado**



Fonte: Autoria própria.

### 3.3 TOR

Até este ponto, a solução fornece uma rede sem fios que provê internet aos seus clientes por meio de qualquer dispositivo ligado as portas USB ou Ethernet.

O passo seguinte da solução de anonimização, é a configuração e adaptação do serviço Tor para cada um dos clientes por meio da rede sem fios. Se bem existe infinidade de procedimentos documentados na internet, este trabalho foi inspirado na recopilção de passos explicados na palestra do grupo de pesquisas de segurança Bxsec no marco da Bside São Paulo 2018.

Para a instalação do serviço Tor é preciso atualizar os repositórios e pacotes de software à ultima versão.

```
$ sudo apt-get update
$ sudo apt-get upgrade
```

Seguidamente, se instala o serviço.

```
$ sudo apt-get install tor
```

Para a configuração de Tor é necessário criar e modificar o arquivo do serviço “torc”, por meio da instrução:

```
$ sudo nano /etc/tor/torc
```

A continuação se deve copiar o seguinte conteúdo com os parâmetros necessários para a correta execução de Tor, de acordo com a documentação provida por a *Tor foundation* (TOR, 2018d):

```
1. #Arquivo Logs
2. Log notice file /var/log/tor/notices.log
3. #Interface virtual Rango IPs
4. VirtualAddrNetwork 10.192.0.0/10
5. #Abrir URL tipo .onion e .exit
6. Automapfixes .onion,.exit
7. AutomapHostOnResolve 1
8. TransPort 9040
9. TransListenAddress 192.168.100.1
10. DNSPort 53
11. DNSListenAddress 192.168.100.1
```

Na linha 2, é adicionada a rota do arquivo que armazenará os lógicos dos sucessos. A linha 4, agrega o endereço IP da rede virtual criada para o gerenciamento do tráfego de Tor e seus circuitos virtuais.



A possibilidade de abrir de forma nativa os endereços de serviços ocultos tipo “.onion” ou “.exit”, é adicionada na linha 6. A linha 7 tem o parâmetro com valor de 1, que dizer isto, que Tor é obrigado a mapear um endereço virtual não utilizado para resolver um serviço do tipo *onion* ou qualquer um que fosse expressado nas linhas anteriores. Nas linhas seguintes são indicadas as portas de conexão e os endereços IP de escuta para os serviços DNS e dos circuitos de Tor para sua configuração como um *proxy* transparente, na rede sem fios local “TorUTFPR”.

### 3.3.1 Corta Fogo para Tor (Iptables)

Se bem nos passos anteriores foi configurada uma parte do corta fogos, agora é necessário adicionar as configurações que permitam que as petições e respostas realizadas pela rede TOR sejam encaminhadas para a rede local.

Para isso, tem que se modificar as tabelas *iptables* para adicionar as linhas NAT de encaminhamento, a configuração é baseada no manual para *Tor transparent proxy* (DIGITAL\_ARMED\_FORCES, 2018), assim:

```
1. $ sudo iptables -t nat -F
2. $ sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport
   22 -j REDIRECT --to-ports 22
3. $ sudo iptables -t nat -A PREROUTING -i wlan0 -p udp --dport
   53 -j REDIRECT --to-ports 53
4. $ sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --syn -
   j REDIRECT --to-ports 9040
```

Para o início da configuração, é preciso ter certeza que que a *string* NAT do firewall se encontra em zeros, por meio da linha 1.

Depois, se adicionam as linhas precisas para conseguir o encaminhamento dos serviços SSH e DNS, assim como o tráfego de entrada e saída coletado pela porta 9040, agindo como *proxy* transparente, isto, até a rede local sem fios “*wlan0*”.

Se verificam se as configurações da tabela NAT foram corretamente adicionadas, com o comando:

```
sudo iptables -t nat -L
```

A resposta a execução dos comandos apresentados deveria ser do tipo apresentado na Figura 15.

**Figura 15 - Resposta NAT iptables**

```

pi@raspberrypi:~$ sudo iptables -t nat -n -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination           tcp dpt:22 redir ports 22
REDIRECT  tcp  --  0.0.0.0/0              0.0.0.0/0             tcp dpt:22 redir ports 22
REDIRECT  udp  --  0.0.0.0/0              0.0.0.0/0             udp dpt:53 redir ports 53
REDIRECT  tcp  --  0.0.0.0/0              0.0.0.0/0             tcp flags:0x17/0x02 redir ports 9040

```

Fonte: Autoria própria.

Por último, só fica salvar as configurações e indicar os arquivos para armazenar os lógicos do serviço Tor. Para salvar as modificações do firewall *iptables*, é utilizado o comando:

```
sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"
```

Seguidamente, se configura o arquivo de registro de lógicos do serviço Tor. Na primeira linha se indica o nome e localização do arquivo, na segunda e terceira se configuram as permissões de leitura e escrita.

```

$ sudo touch /var/log/tor/notices.log
$ sudo chown debian-tor /var/log/tor/notices.log
$ sudo chmod 644 /var/log/tor/notices.log

```

Para finalizar, é iniciado o serviço Tor e verificado seu estado, além disso, é configurado o demônio de início do sistema para ser executado no arranque.

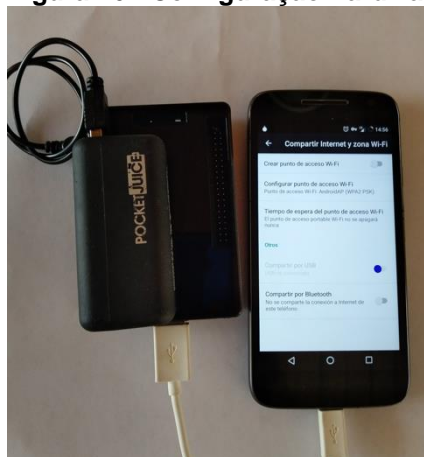
```

$ sudo service tor start
$ sudo service tor status
$ sudo update-rc.d tor enable

```

Neste ponto está finalizada a configuração da solução, para verificar a conexão dos clientes na rede TOR a *Tor Foundation* provê o site <http://check.torproject.org/>. Na Figura 16, observa-se a conexão física do dispositivo utilizado para as provas, fornecendo internet por meio de um aparelho celular.

**Figura 16 - Configuração hardware**



Fonte: Autoria própria.

## 4 CONSIDERAÇÕES FINAIS

Neste capítulo, serão apresentados os resultados evidenciados durante o desenvolvimento da monografia. Além disso, serão explicadas brevemente algumas provas que ajudam a consolidar esses resultados e brindam ao leitor um marco de guia sobre o funcionamento da solução, com bases experimentais.

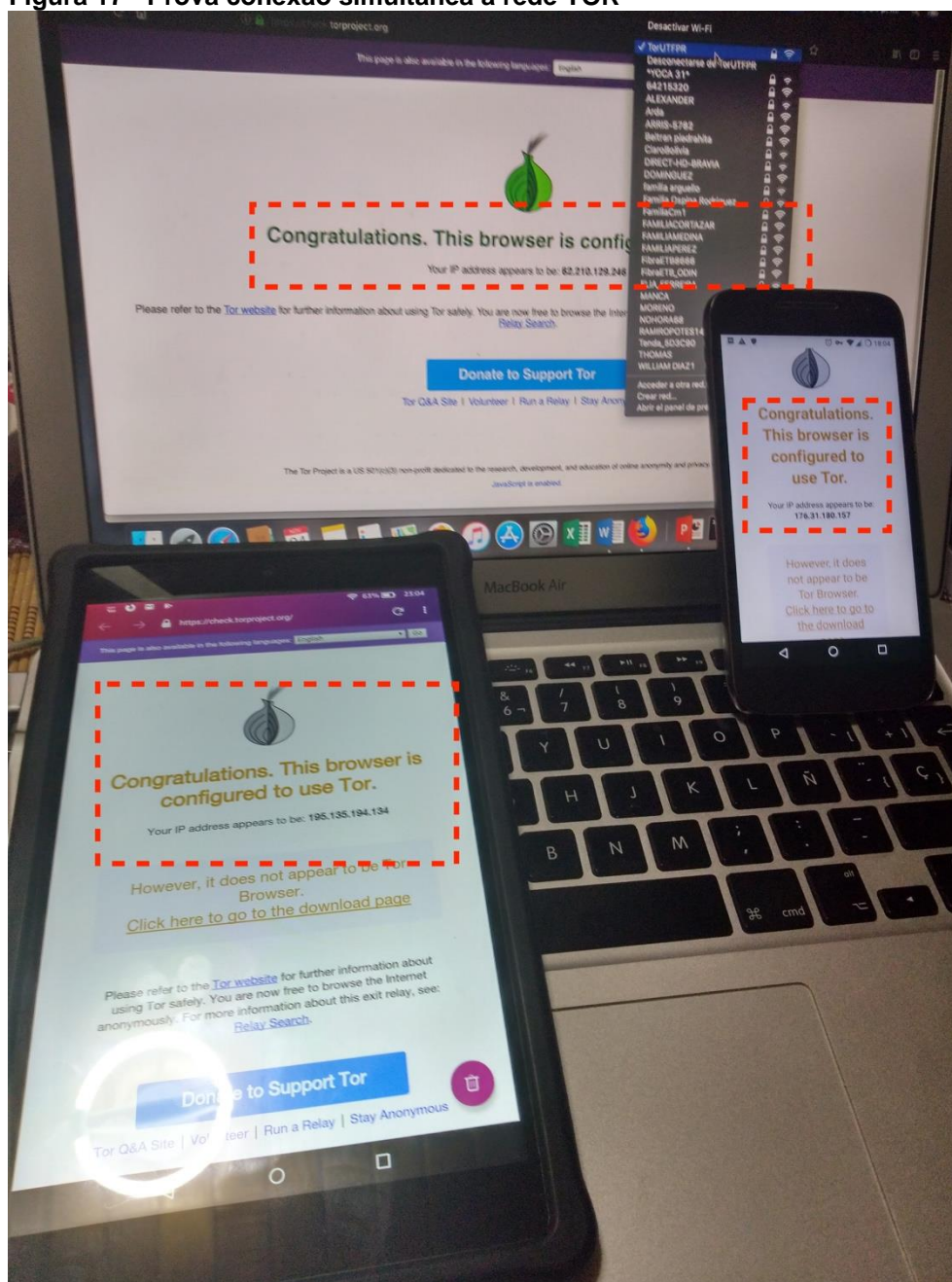
### 4.1 CONCLUSÕES

Durante o percurso da monografia, foi possível evidenciar a versatilidade da solução, além da alta portabilidade que fornece em ambientes difíceis. Para comprovar a funcionalidade do desenho, foram utilizados três dispositivos: um computador portátil, uma *tablet* e um telefone celular.

Em cada um dos dispositivos foi utilizado um navegador da web diferente: no computador, Mozilla Firefox; na *tablet*, Chrome; e no telefone celular, o navegador de *Android*. A ideia, é corroborar que a solução provê a possibilidade de navegação através da rede TOR sem necessidade de alterar nenhum parâmetro dentro do dispositivo e tem funcionalidade independentemente do navegador ou do sistema operativo.

Na Figura 17, é possível observar os três dispositivos conectados á rede local “TorUTFPR” simultaneamente, com os três diferentes navegadores abertos. Apesar disso, foram encaminhados através da rede TOR e, segundo mostra o aplicativo de detecção provido pela *Tor Foundation*, se encontram prontos para a sua utilização nesta rede sem nenhuma configuração adicional.

Figura 17 - Prova conexão simultânea à rede TOR



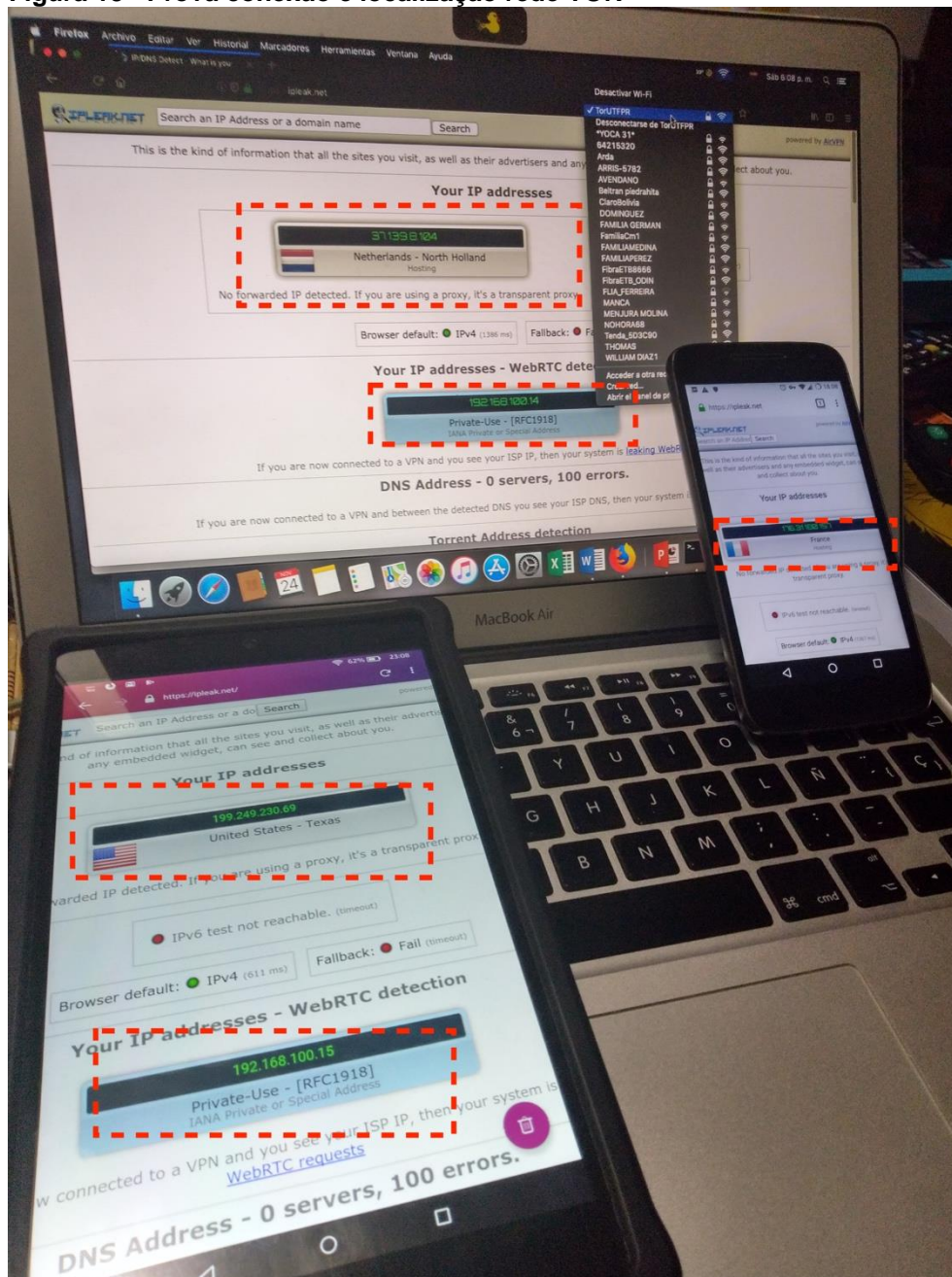
Fonte: Autoria própria.

Outro dos objetivos propostos na hora de empreender este trabalho, foi conseguir que cada um dos clientes conectados à rede local apresentassem uma localização diferenciada, fornecida por um circuito virtual *onion* disposto individualmente para tal fim. Desta forma, poderiam ser detectados em um país diferente, ainda estando na mesma aula.

Na Figura 18, é possível apreciar que cada um dos dispositivos, além de apresentar o endereço IP de rede 192.168.100.0 correspondente à rede local sem fios

wlan0, é detectado por os serviços web de localização em um país diferente, para este caso: Os Estados Unidos, a França e os Países Baixos.

Figura 18 - Prova conexão e localização rede TOR



Fonte: Autoria própria.

Como é evidenciado nas provas, os objetivos do processo de conexão foram alcançados satisfatoriamente. Primeiro, foram conseguidas conexões anônimas para cada um dos dispositivos conectados à rede local. Segundo, foram providas localizações diferenciadas em países aleatórios para cada um deles.

As provas foram feitas com três clientes conectados simultaneamente, cumprindo outro dos objetivos propostos. É importante notar que o número de clientes a suportar está limitado às especificações de memória e de processamento do hardware da *Raspberry Pi*.

O processo de consecução dos elementos para a realização do projeto, é relativamente fácil e economicamente muito viável. Depois de varias provas, baseadas em múltiplos tutoriais e manuais encontrados na internet foi possível chegar a uma configuração estável e funcional que fornece estabilidade e segurança, graças aos métodos e protocolos utilizados. Esta configuração foi explicada minuciosamente durante o capítulo de instalação e configuração do ambiente.

Finalmente, em conclusão, esta solução cumpre com os requerimentos mínimos para fornecer um ambiente de conexão e anonimato de acordo aos objetivos propostos; e eventualmente, poderia ser utilizada em países, povos ou sociedades com problemas de respeito pelos direitos humanos, repressão e censura, que limitem as liberdades e a neutralidade da internet.

Adicionalmente, o autor deixa claridade que o propósito desta monografia é puramente educativo. A utilização dos métodos, códigos ou configurações aqui providas para um uso diferente a este, são responsabilidade de quem as usasse com esse fim.



## REFERÊNCIAS

BERNERS-LEE, Tim. **Information management: A proposal**. Copyright© Tim Berners-Lee, mar. 1989. Disponível em: <<https://www.w3.org/History/1989/proposal.html>>. Acesso em: 17 out. 2018.

BERNERS-LEE, Tim. **Weaving the web: The original design and ultimate destiny of a world wide web by its inventor**. Cambridge: Harper, 1999. p. 226.

BIDDLE, Peter et al. **The Darknet and the future of content distribution**. Microsoft Corporation, consultado em 20 nov. 2018. Disponível em: <<https://crypto.stanford.edu/DRM2002/darknet5.doc>>. Acesso em: 20 nov. 2018.

DEBIAN. **Debian: Manpages**. Debian, 2018. Disponível em: <<https://manpages.debian.org/stretch/ifupdown/interfaces.5.en.html>>. Acesso em: 20 out. 2018.

DIGITAL\_ARMED\_FORCES. 2018. **How to Setup Tor as transparent proxy**. Copyright© Digital Armed Forces, 2018. Disponível: <<http://digitalarmedforces.org/index.php/8-linux/19-how-to-setup-tor-as-a-transparent-proxy-on-ubuntu-linux>>. Acesso em: 20 out. 2018.

FERNÁNDEZ, David Lorenzo Morillas. **Introducción a la criminología**. Revista de Derecho Español, n. 8, 2004. p. 29-60. Disponível em: <<https://www.lamjol.info/index.php/DERECHO/article/view/978>>. Acesso em: 10 nov. 2018.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. Porto Alegre: Mc Graw Hill, 2010. p. 15-16.

GOLDSCHLAG, David M.; REED, Michael G.; SYVERSON, Paul F. **Hiding routing information**. Workshop on Information Hiding, Cambridge, Reino Unido, mai. 1996. Disponível em: <<https://www.onion-router.net/Publications/IH-1996.pdf>>. Acesso em: 17 out. 2018.

GÓMEZ, Francisco Periañez. **Tutorial del servicio DHCP**. Instituto de Educación Superior de Mar de Cádiz, publicado em: 01 set. 2013. Disponível em: <<http://fpg.site11.com/DHCP/defaultleasetime.html>>. Acesso em: 18 out. 2018.

GOOGLE. **Googlebot**. Copyright© Google, 2018. Disponível em: <<https://support.google.com/webmasters/answer/182072?hl=en>>. Acesso em: 11 out. 2018.

JUNIPER. **Juniper Documentation**. Copyright© 1999-2018 Juniper Networks, Inc, publicado em: 30 ago. 2018. Disponível em: <[https://www.juniper.net/documentation/en\\_US/junos/topics/concept/interface-security-loopback-understanding.html](https://www.juniper.net/documentation/en_US/junos/topics/concept/interface-security-loopback-understanding.html)>. Acesso em: 20 out. 2018.

KAHN, Robert; CERF, Vinton. **A protocol for packet network intercommunication**. In: IEEE Transactions on Communications, v. 22, n. 5, mai. 1974, p. 637-648. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/1092259>>. Acesso em: 17 out. 2018.

LAMBERT, Laura et al. **Internet: A historical encyclopedia**. Oxford, California: ABC-CLIO, 2005.

LAUTENSCHLAGER, Steve. 2016. **Surface web, Deep web, Dark web: Whats the difference**. Copyright © 2002-2018 CambiaResearch.com, publicado em: 06 fev. 2016. Disponível em: <<https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web---whats-the-difference>>. Acesso em: 15 out. 2018.

LICKLIDER, J. C. R. **Man-computer symbiosis**. 1960. IRE Transactions on Human Factors in Electronics, 1960, p. 4-11.

LICKLIDER, J. C. R.; CLARK, Welden E. **Online man computer and communications**. 1962. AIEE-IRE '62 (Spring) Proceedings, São Francisco, California, 1962, p. 113-128. Disponível em: <<https://dl.acm.org/citation.cfm?id=146084>>. Acesso em: 17 out. 2018.

LICKLIDER, J. C. R.; TAYLOR, Robert W. **The computers as a communications device**. 1968. Science and Technology, 1968, p. 21-40.

MALINEN, Jouni. **Hostapd documentation**. Jouni Maline, 2016. Disponível em: <<https://w1.fi/cgiit/hostap/plain/hostapd/hostapd.conf>>. Acesso em: 20 out. 2018.

NETFILTER. **The netfilter.org project**. The netfilter.org project, 2018. Disponível em: <<https://www.netfilter.org/>>. Acesso em: 18 out. 2018.



PHILLIPS, Sarah. **A brief history of Facebook**. Copyright© Guardian News and Media Limited, publicado em: 25 jul. 2007. Disponível: <<https://www.theguardian.com/technology/2007/jul/25/media.newmedia>>. Acesso em: 17 out. 2018.

PILIOURAS, Teresa C. Mann. **Network design: Management and technical perspectives**. 2. ed. Boca Raton, Florida: CRC Press, 2004.

RASPBERRY. **Raspberry Pi 3 Model B**. RS Components, visitado em: 20 out. 2018a. Disponível em: <<https://docs-emea.rs-online.com/webdocs/165e/0900766b8165e389.pdf>>. Acesso em: 20 out. 2018.

RASPBERRY. **Setting up a Raspberry Pi as a wi-fi access point**. Copyright© ENGINEERED IN NYC Adafruit, 2018b. Disponível em: <<https://learn.adafruit.com/setting-up-a-raspberry-pi-as-a-wifi-access-point/install-software>>. Acesso em: 18 out. 2018.

RASPBIAN. **Welcome to Raspbian**. Raspberry Pi Foundation, 2018. Disponível em: <<https://www.raspbian.org/>>. Acesso em: 17 out. 2018.

RHEL. **Red Hat Enterprise Linux 4: Manual de referencia**. Capítulo 18: Iptables, Red Hat Enterprise Linux Documentation (RHEL), 2005. Disponível em: <<http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-iptables-options.html>>. Acesso em: 20 out. 2018.

ROBERTS, Lawrence G. **Resource sharing computer networks**. Advanced Research Projects Agency, 1968.

ROMERO, Mario Lobo. **Un paseo por la deep web**. Universitat Oberta de Catalunya, Barcelona, Espanha, publicado em: jan. 2018. Disponível em: <<http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72626/7/mloboromTFM0118memoria.pdf>>. Acesso em: 17 out. 2018.

TOMLINSON, Ray. **The first message (email)**. Ray Tomlinson, 2018. Disponível em: <<https://openmap.bbn.com/~tomlinso/ray/firstemailframe.html>>. Acesso em: 17 out. 2018.

TOR. **Tor's protocol specifications**. TOR Project Fundation, 2018c. Disponível em: <<https://gitweb.torproject.org/torspec.git/tree/dir-spec.txt>>. Acesso em: 17 out. 2018.

TOR. **Tor: Documentation.** TOR Project Foundation, 2018d. Disponível em: <<https://www.torproject.org/docs/tor-manual.html.en>>. Acesso em: 20 out. 2018.

TOR. **Tor: Metrics.** TOR Project Foundation, 2018b. Disponível em: <<https://metrics.torproject.org/rs.html#search/flag:Authority>>. Acesso em: 17 out. 2018.

TOR. **Tor: Overview.** TOR Project Foundation, 2018a. Disponível em: <<https://www.torproject.org/about/overview.html.en>>. Acesso em: 17 out. 2018.

USERS. **Top 10 countries by possible censorship events.** Copyright© The TOR Project, pesquisa em: 30 set. 2018. Disponível em: <<https://metrics.torproject.org/userstats-censorship-events.html>>. Acesso em: 17 out. 2018.