Equipamentos de Duplicação Forense

Trabalho de Conclusão de Curso

Autor: Erick Martinez

INSTITUTO DE PÓS-GRADUAÇÃO E GRADUAÇÃO

IPOG

COMPUTAÇÃO FORENSE E PERÍCIA DIGITAL

ERICK NEVES MARTINEZ

EQUIPAMENTOS DE DUPLICAÇÃO FORENSE

RIO DE JANEIRO

2019

ERICK NEVES MARTINEZ

EQUIPAMENTOS DE DUPLICAÇÃO FORENSE

Trabalho solicitado para o curso de Computação Forense e Perícia Digital, do Instituto de Pós-Graduação e Graduação – IPOG.

RIO DE JANEIRO

2019

Erick Neves Martinez

EQUIPAMENTOS DE DUPLICAÇÃO FORENSE

Relatório final apresentado à banca examinadora do Instituto de Pós-Graduação e Graduação – IPOG, como parte das exigências para a obtenção do título de pós-graduado na área de Computação Forense e Perícia Digital.

Rio de Janeiro, 17 de março de 2019.

BANCA EXAMINADORA

_____
PROFESSOR ORIENTADOR

_____
PROFESSOR AVALIADOR

_____
PROFESSOR AVALIADOR

AGRADECIMENTOS

Em primeiro lugar a Deus por sempre estar ao meu lado, a todos os amigos e em especial a minha esposa Marianne Fernandes e minha mãe Solange de Moraes por estarem sempre ao meu lado.

Aos professores da instituição IPOG por terem passado o conhecimento e vivencia na área de perícia computacional.

RESUMO

A facilidade da internet e formas de propagar a informação através dela pelo mundo fez com que houvesse um aumento de crimes cibernéticos, entre eles destacam-se pedofilia infanto-juvenil e comércio ilegal, entre outros e com isso tornou-se difícil realizar coleta e análise do material apreendido, gerando grandes atrasos e dificultando a resolução de casos. Nos dias atuais existem diversas empresas que disponibilizam equipamentos de duplicação (cópia de dispositivo) e softwares capazes de realizar atividades forense a um custo muita das vezes elevado e não se sabe exatamente como funciona o código, onde instituições ou empresas que necessitam destas soluções não dispõem de recursos monetários para aquisição. Desta forma, o presente estudo tem por objetivo criar e desenvolver uma solução de baixo custo e a utilização de softwares de código aberto desenvolvidos para facilitar a coleta e análise do material apreendido. Metodologia: foi utilizado o Raspberry Pi 3 b+ para desenvolver um equipamento de baixo custo visando auxiliar na criação de imagens de dispositivos de armazenamento. Como especificação do tema proposto, são destacados equipamentos existentes e a criação de um para ajudar peritos de todo o mundo a realizar a atividade com custo baixo. Resultado: utilização do equipamento proposto traz eficiência, baixo custo e facilidade de gerar imagens de equipamentos apreendidos. Conclusão: os equipamentos apresentados são na verdade uma caixa com vários recursos que podem ser facilmente implementados e/ou criados utilizando o Raspberry Pi 3 b+ juntamente com a distribuição Kali Linux.

Palavras-Chave: Raspberry, forense, cibernéticos, internet, equipamento, pedofilia.

ABSTRACT

The ease of the internet and ways to spread the information through the world has caused an increase in cyber crimes, among them pedophilia and child trafficking, among others, and it has become difficult to perform collection and analysis of the material seized, causing great delays and making case resolution difficult. Nowadays there are several companies that offer duplication equipment (copy of device) and software capable of performing forensic activities at a high cost many times and it is not known exactly how the code works, where institutions or companies that need these solutions do not have of monetary resources for acquisition. In this way, the present study aims to create and develop a low cost solution and the use of open source software developed to facilitate the collection and analysis of the seized material. Methodology: Raspberry Pi 3 b + was used to develop a low cost device to aid in the imaging of storage devices. As a specification of the proposed theme, existing equipment is highlighted and the creation of one to help experts from all over the world to carry out the activity at low cost. Result: use of the proposed equipment brings efficiency, low cost and easy to generate images of seized equipment. Conclusion: The devices presented are actually a box with several features that can be easily implemented and / or created using Raspberry Pi 3 b + along with the Kali Linux distribution.

Keywords: Raspberry, forensics, cyber, internet, equipment, pedophilia.

SUMÁRIO

1. INTRODUÇÃO

A facilidade da internet e formas de propagar a informação através dela pelo mundo fez com que houvesse um aumento de crimes cibernéticos, entre eles destacam-se pedofilia infanto-juvenil e comércio ilegal, entre outros e com isso tornou-se difícil realizar coleta e análise do material apreendido, gerando grandes atrasos e dificultando a resolução de casos. Nos dias atuais existem diversas empresas que disponibilizam equipamentos de duplicação (cópia de dispositivo) e softwares capazes de realizar atividades forense a um custo muita das vezes elevado e não se sabe exatamente como funciona o código, onde instituições ou empresas que necessitam destas soluções não dispõem de recursos monetários para aquisição.

Segundo Rodrigo dos Santos Bacelar Gouveia Barbosa e Luiz Eduardo Marinho Gusmão (2015, p. 95),

> O procedimento de cópia forense pode ser realizado com a utilização de equipamentos especializados ou por meio de computadores comuns, auxiliados por programas de duplicação.

A carência por este tipo de pesquisa é grande, visto que muitas vezes a facilidade de adquirir um equipamento de duplicação forense se torna mais fácil do que desenvolver um. Por este motivo esta pesquisa tem como objetivo apresentar uma solução de baixo custo para ajudar a todos os peritos a realizarem uma cópia segura dos dados a serem analisados.

2. MATERIAL E MÉTODOS

Foi realizado uma pesquisa bibliográfica com intuito de criar um equipamento de duplicação de dados que seja eficaz com baixo custo, estendendo-se futuramente ao desenvolvimento de outras soluções para perícia computacional.

Embora existam diversos equipamentos de diferentes empresas que atuam na criação de equipamentos de duplicação de dados, este trabalho consiste em desenvolver um equipamento de baixo custo e com flexibilidade de explorar mais recursos no processo ilustrado na tabela 1.

Após uma pesquisa de preços realizada em diversas lojas (Mercado Livre, Americanas e Gearbest), foram encontrados alguns valores mais acessíveis como mostra a tabela abaixo.

EQUIPAMENTO	QUANTIDADE	CUSTO
Raspberry Pi 3 b+	1	R$ 178,00.
Display touch	1	R$ 93,00.
Dock Station	2	R$ 86,00.
Distribuição Kali Linux	1	R$ 0.
Software Etcher	1	R$ 0.
Cartão de memória 64GB	1	R$ 19,85.
	Total:	R$ 462,85

Tabela 1 – Lista de equipamentos e valores.

Conforme a tabela acima, o custo de montar um equipamento de duplicação é baixo. Requer apenas conhecimento do hardware e software.

3. DESENVOLVIMENTO

3.1. O que é computação forense

A computação forense é uma arte de descobrir e recuperar informações sobre um crime de tal forma a torna-lo admissíveis em tribunal (YASINCAC, MANZANO, 2001). Segundo Pedro Monteiro da Silva Eleutério e Marcio Pereira Machado a computação forense tem como objetivo principal determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhe validade probatória em juízo.

3.2. O que é duplicação de dados e hash

Duplicação de dados (espelhamento) é o ato de copiar bit a bit (é a menor unidade de informação que pode ser armazenada ou transmitida e pode assumir apenas 2 valores: 0 ou 1) um arquivo de um local para outro mantendo sua integridade. Segundo Pedro Eleutério e Marcio Machado (2011, p. 55),

> O espelhamento é uma técnica que consiste na cópia exata e fiel dos dados (bit a bit) contidos em um dispositivo de armazenamento computacional para outro.

Este é uma das etapas para a análise chamada de Coleta ou Preservação. Segundo Jesus Velho (2015, p. 93),

> A fase de preservação também compõe o processo de cadeia de custódia, que trata do registro cronológico de manuseio da evidência, desde sua coleta até o fim do procedimento em que está inserido.

A imagem a seguir exemplifica o processo de um método bastante utilizado pelos peritos.

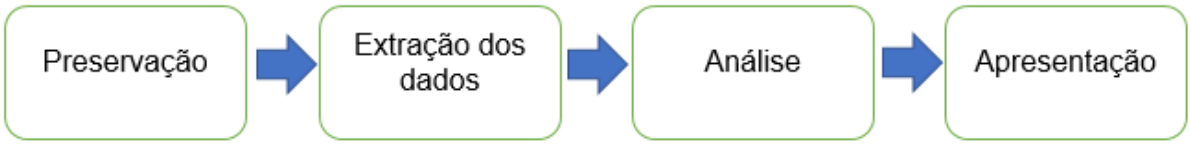


Imagem 1 – Fases básicas do exame pericial de mídias computacionais.

Segundo Jesus Velho (2015, p. 91),

> “A primeira fase, a Preservação, tem como principal objetivo garantir que a evidência digital não sofra alteração durante a realização do exame. A etapa seguinte, a Extração dos dados, visa a identificar os arquivos ou fragmentos de arquivos presentes na mídia. Por sua vez, o propósito da terceira etapa, a

> Análise, é identificar nos arquivos recuperados informações úteis ao fato que está sob investigação. E, por fim, a etapa de Apresentação é o modo como o perito irá formalmente relatar suas conclusões ao final dos exames. Em outras palavras, essa última etapa, é o laudo ou outro documento técnico que será elaborado..."

Em uma análise forense, o(s) dado(s) copia(dos) só serão válidos em juízo se estes mantiverem íntegros, a forma de um perito comprovar a integridade é através do hash.

Segundo Petter Lopes (2013),

> O uso das funções de Hash (mais indicado o SHA) é um dos métodos mais utilizados para verificação de integridade dos dados, gerando uma sequência de números obtidos através de algoritmos matemáticos que identificam os dados ou a imagem pericial de forma única.

3.3. Duplicadores de dados via software

São softwares que realizam espelhamento de dados. Sua utilização irá depender da situação que o perito se encontra ao realizar o processo de coleta de evidências.

Entre as soluções existentes são destacados:

- dd.
- FTK Imager.
- EnCase.

Entre outros.

O comando dd destaca-se por ser nativo do sistema operacional baseado em Linux, logo qualquer distribuição Linux deverá ter o comando já instalado, mas as demais soluções também realizam a mesma ação, sendo necessário a instalação.

3.4. Duplicadores de dados via hardware

Duplicadores de dados via hardware são dispositivos físicos que possuem internamente um sistema e/ou programações pré-definidas para realizar o espelhamento de mídias.

Uma das principais diferenças entre os equipamentos está na capacidade de reconhecimento de mídias. Este por sua vez é um dos fatores que irá interferir diretamente no valor do equipamento.

A tabela a seguir contém a exemplos de empresas e seus respectivos equipamentos de duplicação de dados. Os valores apresentados foram retirados do site e https://siliconforensics.com.

EMPRESA	NOME DO EQUIPAMENTO	CUSTO
Wiebetech	Ditto DX forensic Fieldstation	US$: 2.249,00.
Media Clone	Supercopier IT 8” T3 SAS	US$: 4.149,00.
Logicube	WriteProtect Desktop	US$: 1.199,00.

Tabela 2 – Lista de equipamentos de duplicação de dados.

A seguir são apresentados os equipamentos de duplicação de dados listados na tabela 3.

		
Imagem 2 - FAU II – WriteProtect Desktop.	Imagem 3 - FAU II – Supercopier IT 8” T3 SAS.	Imagem 4 – Ditto DX forensic Fieldstation.

Tabela 3 – Imagens de equipamentos.

3.5. Sistemas Operacionais forenses

Segundo Jesus Velho (2015, p. 98),

> Há sistemas operacionais de código livre e com viés forense que trazem consigo um conjunto de softwares direcionados ao trabalho pericial, como o já mencionado TSK.

Na tabela 2, são apresentados os principais sistemas operacionais utilizados para duplicação de dados. Lembrando que é importante manter a integridade dos dados na mídia apreendida e nem todos os sistemas operacionais possuem a preocupação em manter o disco integro. Sistemas operacionais voltados para perícia tem essa preocupação em manter o estado atual integro. Segundo Jesus Velho (2015, p. 96),

> Essa atenção é necessária para identificar a presença das áreas latentes conhecidas como HPA (host Protected Area) e DCO (Device Configuration OverLay).

SISTEMA OPERACIONAL	DISTRIBUIÇÃO
Linux	Kali Linux
Linux	C.A.I.N.E
Linux	DEFT
Windows	WinFE

Tabela 4 – Lista de Sistemas Operacionais.

Grande parte dos sistemas operacionais listados na tabela 4 são Live CD, significando que não necessitam de instalação, rodam diretamente do CD ou outro dispositivo, como por exemplo Kali Linux que pode ser instalado em um pen drive.

3.6. Desenvolvendo um equipamento de duplicação de baixo custo

A seguir será apresentado a construção do equipamento de duplicação de baixo custo. Os equipamentos e métodos foram apresentados no capítulo 2. A montagem do Raspberry Pi 3 b+ é simples e acompanha manual de instalação na case.

Será utilizado o software Etcher para realizar a gravação da imagem do Kali Linux no cartão de memória. O mesmo poderá ser baixado no site do fabricante: https://www.balena.io/etcher/. Após realizar o download e instalar no computador, será necessário iniciar o programa. A imagem a seguir apresenta o software iniciado.

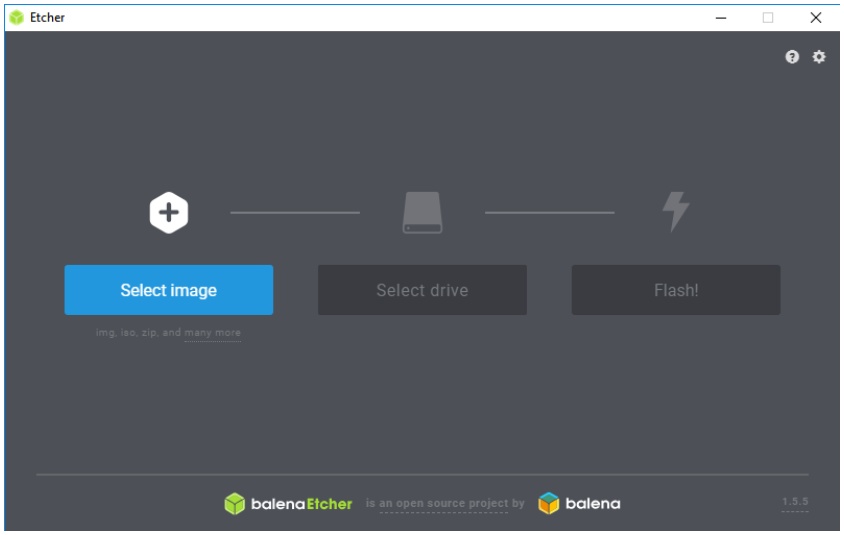


Imagem 5 – Etcher iniciado.

Para baixar a imagem do Kali Linux, acesso a URL: https://www.offensive-security.com/kali-linux-arm-images/. A versão utilizada foi a 2019.1.

Retorne para o Etcher e clique em Select image, localize a imagem e em seguida clique em Abrir. Após selecionar a imagem será necessário informar o local aonde será gravado conforme imagem a seguir.

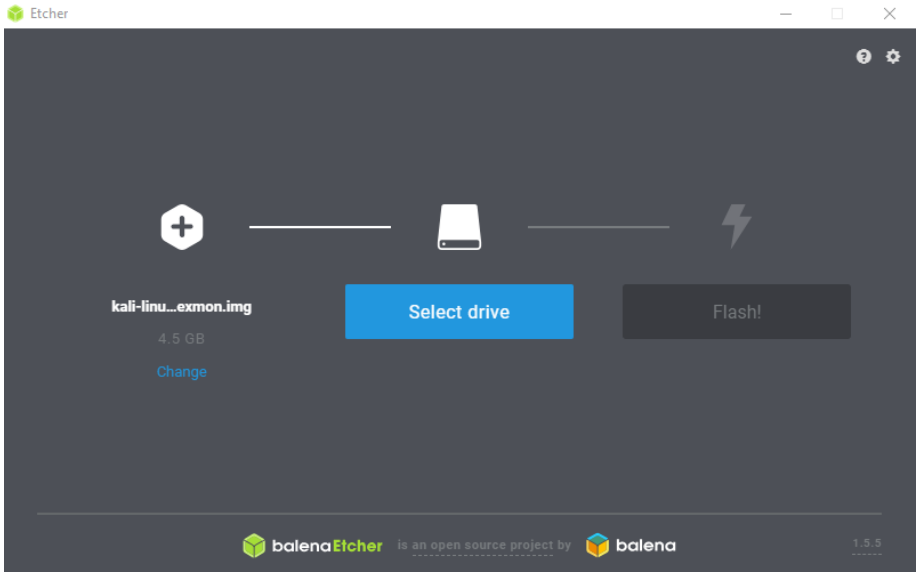


Imagem 6 – Etcher selecionando local de gravação.

Após adicionar a imagem do Kali Linux clique em Flash.

Diante da imagem no pendrive, conecte no Raspberry e ligue o dispositivo. O processo de instalação do Kali Linux no dispositivo é igual de instalação em um computador convencional. Serão solicitadas informações de configurações de região, senha, entre outros. As imagens a seguir apresentam o processo de instalação.

Imagem 7 – Iniciando o processo de instalação.

Processo inicial ao reconhecer o dispositivo conectado. Deverá ser selecionado a opção *Install* para dar início ao Kali Linux.

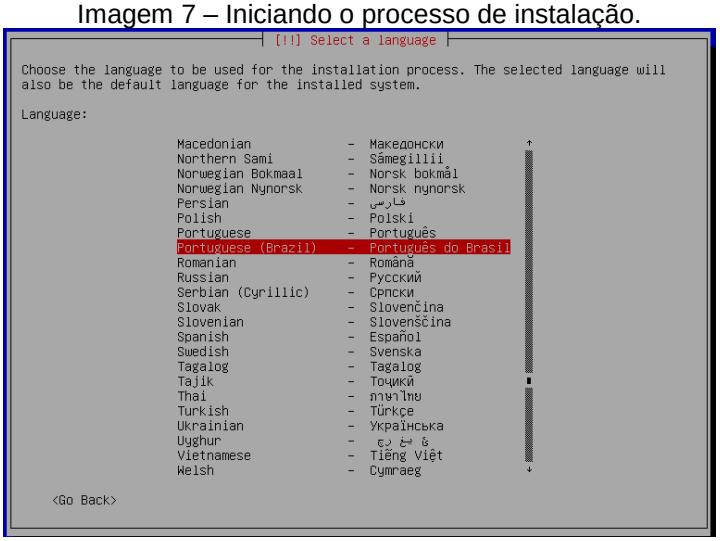


Imagem 8 – Seleção de idioma do sistema operacional.

A primeira configuração a ser realizada será a seleção da linguagem para a instalação do Kali Linux. Será utilizado *Portuguese (Brazil)*.

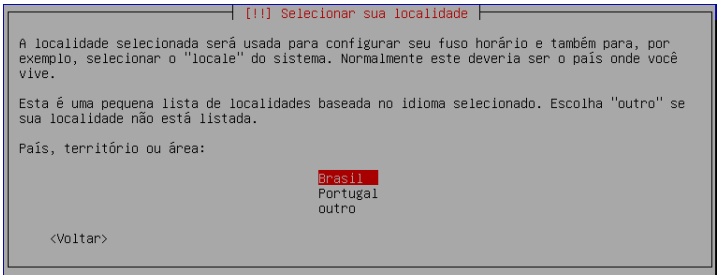


Imagem 9 – Seleção de localidade.

Selecione a localidade correta. Será utilizado *Brasil*.

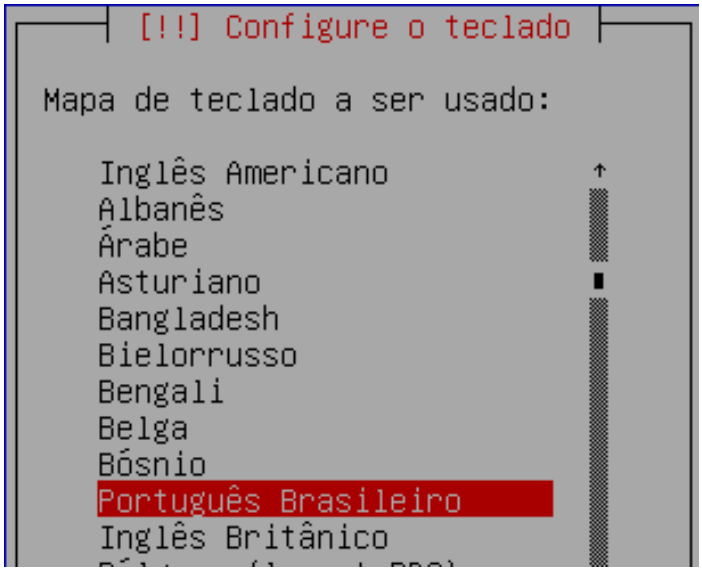


Imagem 10 – Seleção do teclado.

A seguir será necessário informar o tipo de teclado a ser utilizado. Será utilizado *Português Brasileiro*.

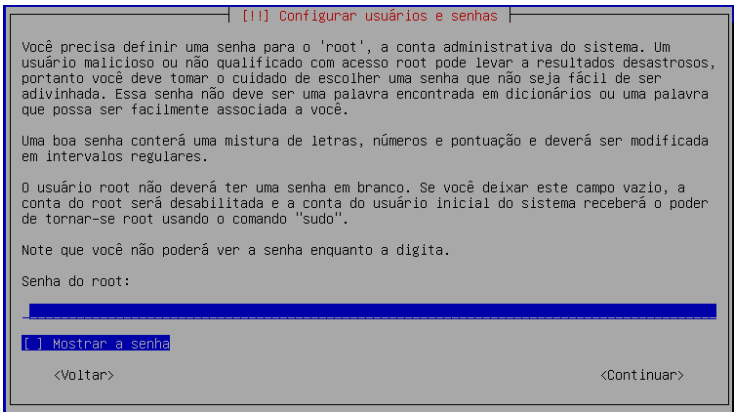


Imagem 11 – Seleção de senha.

Será necessário informar a senha do usuário administrativo, conhecido como *root* no .

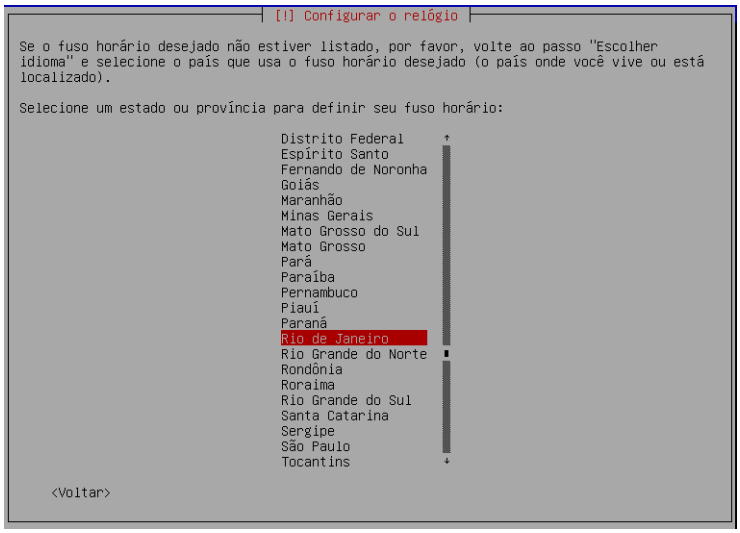
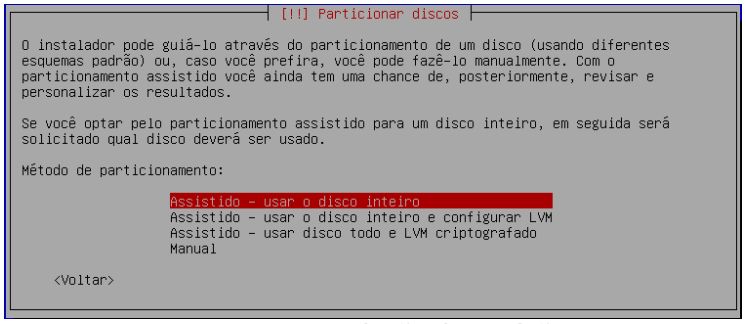


Imagem 12 – Seleção de fuso horário.

Será necessário informar o fuso horário. Será selecionado *Rio de Janeiro*.



Será necessário definir as partições do sistema.

Imagem 13 – Criação de partição.

Com o sistema já instalado e configurado o perito poderá utilizar o dispositivo com auxílio da case. A distribuição Kali Linux dá suporte a diversas ferramentas para a realização da duplicação de dados, como por exemplo IPED, dd, entre outros.

Anexado um script desenvolvido em Shell Script para auxiliar no processo de criação de imagem. Este utiliza o comando o comando dd para efetuar a atividade de duplicação de dados.

4. CONSIDERAÇÕES FINAIS

A partir do trabalho apresentado, é possível concluir que os equipamentos existentes (comerciais) e o proposto realizam as mesmas atividades de duplicação de dados. Diferente das soluções apresentadas, o custo benefício é grande além possibilitar a utilização do dispositivo criado em outras atividades de perícia, como por exemplo a utilização de outras ferramentas para examinar a mídia duplicada.

Por fim, este trabalho buscou apresentar de forma clara e objetiva os equipamentos existentes no mercado e apresentar a possibilidade de criação de um, com foco na duplicação de dados, buscando ajudar os peritos a terem seu próprio equipamento.

5. REFERÊNCIAS

VELHO, Jesus Antônio. **Tratado de Computação Forense.** 1ed. Rio de Janeiro: Millennium, 2016.

ELEAUTÉRIO, Pedro Monteiro da Silva; MACHADO, Márcio Pereira. **Desvendando a Computação Forense.** 1. ed. Rio de Janeiro: Novatec, 2011.

FARMER, Dan. **Perícia Forense Computacional. Teoria e Prática Aplicada.** 1. ed. Rio de Janeiro: Pearson Prentice Hall, 2006.

VECCHIA, Evandro Della. **Perícia Digital. Da Investigação à Análise Forense.** 1. ed. Rio de Janeiro: Millennium, 2014.

COSTA, Marcelo Antônio Sampaio Lemos. **Computação Forense.** 3. ed. Rio de Janeiro: Millennium, 2011.

BARROS, Aidil Jesus da Silveira; LEHFELD, Neide Aparecida de Souza. **Fundamentos da Metodologia Científica.** 3. ed. São Paulo: Pearson Prentice Hall, 2007.

ANEXO

SCRITP DE DUPLICAÇÃO DE DADOS