CBP

CENTRO BRASILEIRO
DE PERÍCIA

MANIFESTAÇÃO TÉCNICA REFERENTE AO LAUDO DE PERÍCIA CRIMINAL FEDERAL 0335/2018

Índice

1. Objetivo

O objetivo desde documento é a elaboração de manifestação técnica referente ao Laudo de Perícia Criminal Federal 0335/2018 – SETEC/SR/PF/PR.

2. Síntese

O Laudo de Perícia Criminal Federal 0335/2018, foi elaborado através da análise de 11 HDs e 2 Pendrives, fornecidos pela empresa Odebrecht S/A, através de 4 entregas.
O principal objetivo da perícia foi analisar o funcionamento dos sistemas Drousys e My Web Day, utilizados pelo Grupo Odebrecht, e responder aos quesitos.

Essa manifestação é baseada somente na análise do Laudo Pericial, e consulta a outros documentos disponibilizados pelo solicitante, Claudio Wagner.

3. Do Correto Procedimento para Aquisição de Dados

O trabalho executado pelo MPF e pelos peritos da Polícia Federal baseia-se exclusivamente no exame de mídias digitais, e portanto devem seguir, **rigorosamente**, o procedimento forense de duplicação dessas mídias, recomendado pelo MPF, para posterior análise.

O **Ministério Público Federal**, no livro **Roteiro de Atuação Sobre de Crimes Cibernéticos** (de uso restrito às autoridades da Justiça brasileira, incluindo a Polícia Federal, Polícia Civil, Procuradores da República, Juízes Federais, Promotores de Justiça), aplicável ao caso por se tratar de exame de material digital, define no Capítulo 3 que:

> Os métodos consolidados na ciência forense são igualmente adotados na investigação de crimes na Internet. Tais métodos consistem basicamente na **aquisição, preservação, análise e apresentação de evidências.** Estes quatro passos envolvem uma série de atores e atividades criteriosas e na prática costumam ser cíclicos. Vê-se raramente casos em que a apresentação de evidências é única e

> definitiva. O exercício do contraditório possibilita que a defesa conteste a legitimidade dos procedimentos de investigação ou mesmo a consistência de um laudo pericial, tornando usual a necessidade de novas aquisições, análises e apresentação das informações durante o andamento do processo.
>
> **É necessário cumprir com alguns requisitos para que as evidências digitais de uma investigação sejam juridicamente válidas.** Segundo a RFC 3227[1], que oferece uma série de recomendações para procedimentos de coleta e preservação de provas em meio digital...

A aquisição é o ponto de partida da investigação, e a recomendação para a coleta de informação, tem definido como um dos itens da RFC 3227 a questão da confiabilidade do dado analisado.

> **Confiável: não deve haver incertezas acerca da autenticidade e veracidade das evidências, bem como sobre as formas como foram coletadas e posteriormente manuseadas durante a investigação.** (tradução livre)

Fica claro que a clonagem e geração do Hash é fundamental no procedimento de análise de mídias, sem o qual todos e os demais procedimentos definidos no **Roteiro de Atuação Sobre de Crimes Cibernéticos do Ministério Público Federal**, ficam comprometidos.

Em resumo, se a aquisição não seguiu os procedimentos forenses, toda cadeia posterior fica prejudicada.

O **Ministério da Justiça**, através da Secretaria Nacional de Segurança Pública define no livro **Procedimento Operacional Padrão – Perícia Criminal**, no Capítulo 3, como deve ser efetuado o Exame Pericial de Mídia de Armazenamento Computacional. Descreve que a finalidade do procedimento é de orientar o profissional de perícia da área de informática a realizar exames que envolvam dados contidos em mídias de armazenamento computacional.

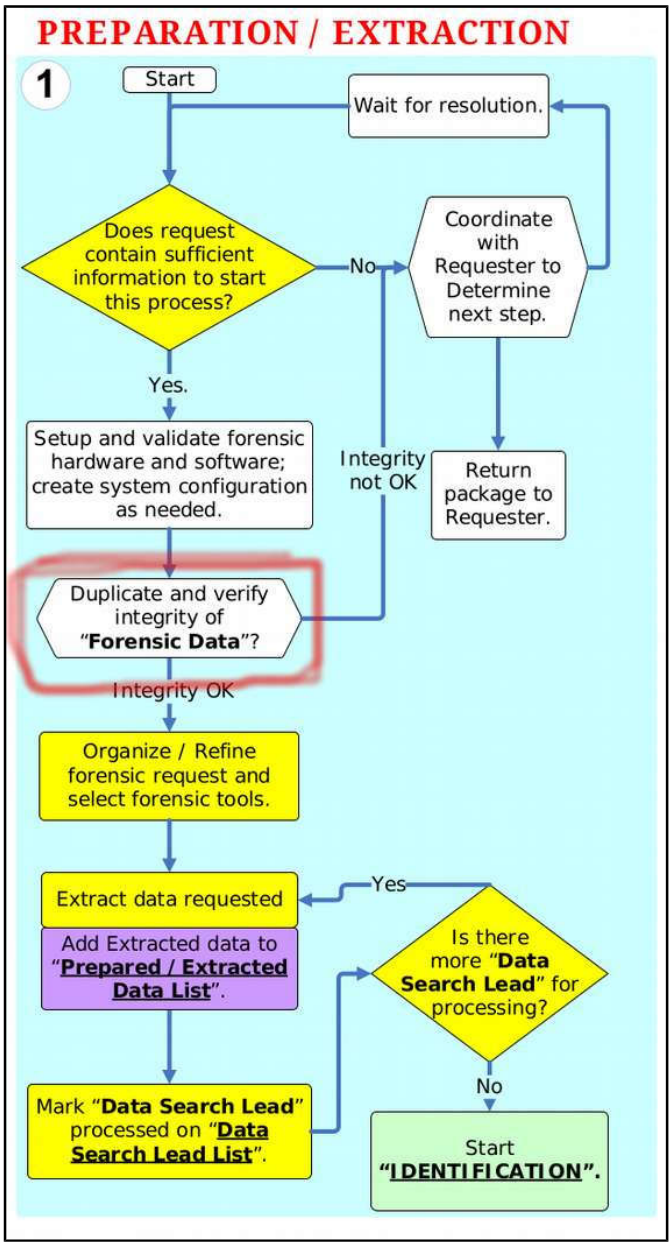
1 **RFC** (acrônimo em inglês de ***R**equest **f**or **C**omments*) ou (ou "pedido para comentários" em português),as RFCs são documentos técnicos desenvolvidos e mantidos pelo IETF (Internet Enginnering Task Force), instituição que especifica os padrões que serão implementados e utilizados em toda a internet.

O parágrafo 4.2 Duplicação de Dados, estabelece que:

> Esta etapa visa a duplicar os dados contidos na mídia original para uma mídia de trabalho de forma a garantir a preservação dos dados.
>
> • O exame deve ser efetuado sobre a cópia. Somente em caso de inviabilidade de realização de cópia deve o exame ser realizado diretamente na mídia original.
>
> • Recomenda-se o tipo de duplicação de dados “mídia para arquivo imagem”, em oposição ao tipo “mídia para mídia”, devido à maior flexibilidade para se analisar diversas mídias simultaneamente e à maior facilidade para se manter a integridade dos dados.
>
> • A duplicação pode ser feita de duas formas: por meio de equipamento forense específico para esse fim ou utilizando-se um microcomputador. Neste último caso, é imperativo impedir que ocorra qualquer alteração nos dados da mídia original, utilizando-se bloqueadores de escrita por hardware ou software.

Fica claro que a clonagem e geração do Hash é fundamental no procedimento de busca e apreensão. Note-se também que é recomendado que a duplicação de dados seja feita na **modalidade arquivo-imagem**, em oposição ao tipo **mídia para mídia.**

Já o **Departamento de Justiça Americano** também estabelece metodologia para análise forense digital, (Digital Forensic Analysis Methodology).


PREPARATION / EXTRACTION
1
Start
Wait for resolution.
Does request contain sufficient information to start this process?
No
Coordinate with Requester to Determine next step.
Yes.
Setup and validate forensic hardware and software; create system configuration as needed.
Integrity not OK
Return package to Requester.
Duplicate and verify integrity of "Forensic Data"?
Integrity OK
Organize / Refine forensic request and select forensic tools.
Extract data requested
Yes
Add Extracted data to "Prepared / Extracted Data List".
Is there more "Data Search Lead" for processing?
Mark "Data Search Lead" processed on "Data Search Lead List".
No
Start "IDENTIFICATION".

Novamente se mostra claro que o procedimento de clonagem e geração de Hash é fundamental na aquisição de material a ser examinado.

Os renomados **professores Enos K Mabuto e H.S. Venter, da Universidade de Pretória**, África do Sul descrevem no artigo **State of the Art os Digital Forensic Techniques**, o processo de aquisição e manipulação de imagens que deve ser aceito pelo Poder Judiciário.

> The digital forensic examiner has to follow the **digital forensic process in order for evidence to be admissible in a court of law**. The digital forensic process consists of a number of phases. It is widely accepted that the phase include acquisition, examination, analysis and reporting [7].
>
> This paper however focuses only on digital forensic techniques as applied in the **two most critical phases of the digital forensic process, which are the acquisition and analysis phases**. The authors found that, from the research conducted, these two phases by far require the most need for action by a digital forensic examiner and, hence the reason for our focus on these two phases.
>
> ...
>
> The acquisition phase describes how data will be acquired from different types of digital information sources. **Data has to be acquired in a manner that maintains its integrity and authenticity** [10].
>
> The acquired data has to undergo forensic duplication or sector level duplication. A write blocker should be used in creating duplicates. The write blocker ensures that nothing is written to the original hard drive. Software imaging tools can also be used [11]. With imaging either a physical image (bit-by-bit image) can be created of the entire physical device or a logical image can be created which comprises of active directories and files available to the operating system [10]. **As a way of verifying the integrity of acquired data hashing is used.** A digital hash conducts a mathematical algorithm of a device or file and provides a fingerprint that authenticates that the data has not been tampered or altered, and this fingerprint is maintained within the case file.

Aqui também se destaca que a geração do Hash na aquisição de imagens é fundamental para garantir a integridade do processo, sem o qual não é admissível em processos criminais.

4. Análise da Primeira Entrega

A primeira entrega de HDs tem como origem, material coletado nos servidores situados no Data Center Bahnhoff em Estocolmo, Suécia, obtido pela empresa FRA (Forensic Risk Alliance), que foi contratada pelo escritório de advocacia da Odebrecht nos Estados Unidos, Quinn Emanuel Urquhart & Sullivan.
Supostamente trata-se de cópia do sistema Drousys. A Odebrecht recebeu esse material em Julho e Setembro de 2016

Na folha 14 do Laudo Pericial, foi anexado um Memo da FRA que apresenta diversas inconsistências:

- *No remetente (From: FRA)*

  Não há nenhuma menção de quem da FRA redigiu o Memo. Ninguém assinou o documento. Como verificar a autenticidade desse documento?

- *Data: July 8, 2017*

  O memo foi elaborado mais de 1 ano após a execução dos procedimentos.

- Timeline: *15 Jul 2016 e 25 Ago 2016*

  A clonagem foi efetuada bem antes da assinatura do acordo de leniência.

- *“A forensic collection machine was attached to the target network” (i.e. Um equipamento de captura forense foi conectado à rede local)*

  Não foi identificada nem a natureza, nem a marca, nem o modelo do hardware e/ou software utilizados nos procedimentos de clonagem.

- *“Each of the two Vmware ESXi machine consoles were logged into using the provided root credentials" (i.e. As duas máquinas Vmware foram logadas pela console com credencias administrativas - root)*

  Se ninguém da Odebrecht acompanhou o procedimento, e não havia ninguém técnico presente (de acordo com o próprio Memo), quem forneceu essas credenciais administrativas ("root credentials")?

- *"The NetApp BMC console was assessed (sic) using the provided credentials and the block devices used by the ESXi cluster were identified" (i.e. A console administrativa do equipamento NetApp foi acessada utilizando-se as credenciais fornecidas, e os dispositivos usados pelo cluster ESXi foram identificados.)*
  Quem forneceu as credenciais do storage NetApp?

- *"Each of the block devices used by Vmware ESXi to host virtual machines were imaged using FTK Imager. The captured block devices contained the entire Vmware VMFS filesystem in use by the two hypervisors." (i.e. Cada um dos dispositivos utilizados para hospedar máquinas virtuais no VMWare ESXi foi clonado, usando o FTK Imager. Os dispositivos continham os sistemas de arquivos tipo VMWare VMFS completos que estavam em uso pelos dois hypervisors.)*
  Se foram capturadas imagens forenses, onde estão o hashes?

- *"At that time, it was determined by FRA that the user content was not accessible using the administrator login and permissions were controlled by the users;" (i.e. Nesse momento, foi determinado pela FRA que o conteúdo dos usuários não era acessível utilizando-se um login administrativo, a as permissões eram controladas pelos usuários.)*
  Não procede a afirmação. Seria caótico se os usuários controlassem a segurança e o acesso aos sistemas, e não os seus administradores. Sempre há uma maneira para o administrador sobrepor qualquer limitação criada por um usuário, por definição.

Em seguida descrevem um procedimento absolutamente bizarro para efetuar um backup dos dados para depois extrair o backup. Ora, a única facilidade que a operação de backup poderia adicionar seria o acesso remoto a dados, usando credenciais de administrador de backup. Mas um usuário qualquer com essa mesma permissão (que pode ser gerada pelo Administrador Local ou pelo Administrador de Domínio) poderia fazer o mesmo, a partir que qualquer máquina, incluindo o citado "laptop forense", sem necessidade de uma outra máquina ("Windows 2008R2 server with Backup Eec 2010R3").

Há inconsistências nos volumes descritos. Como um volume com tamanho total de 819GB, sendo que apensa 219GB estavam em uso, poderia gerar um backup lógico de 1TB?

Em 30 de agosto de 2017, o Ministério Público enviou o Relatório de Análise Nº 7/2017 onde destaca que:

> O Ministério Público Federal vem a presença de Vossa Excelência requerer a juntada do Relatório de Análise Nº 007/2017, da Assessoria de Pesquisa e Análise – ASSPA/PRPR (ANEX0 02), em que analisados elementos extraídos do sistema Drousys utilizado pelo Setor de Operações Estruturadas do Grupo ODEBRECHT (ANEXO 03), que são de interesse da presente ação penal.

Já na primeira folha destaca que:

> A Secretaria de Pesquisa e Análise (SPPEA/PGR) recebeu por meio do Termo de Transferência de Informações Confidenciais, datado de 28 de março de 2017, 4 (quatro) discos rígidos contendo 1.781.624 (um milhão setecentos e oitenta e um mil seiscentos e vinte e quatro) arquivos, totalizando 2,67 terabytes de dados.

A Secretaria de Perícias, Pesquisa e Análise SPPEA é subordinada ao gabinete do Procurador-Geral da República e tem a atribuição de auxiliar, técnica e operacionalmente, as atividades institucionais do Ministério Público Federal – MPF. É responsável pelo processamento e análise de dados obtidos por meio de decisão judicial para subsidiar ações jurídicas.

No entanto, os procedimentos definidos pelo Ministério da Justiça para Aquisição de Dados, não foram observados pelos técnicos, que acabaram por contaminar os HDs, alterando seu estado original. Efetuaram uma cópia não forense para analisar os dados sem nenhuma declaração de como foi efetuado o trabalho, não há nem descrição e nem informações sobre *Hash*.

Para efetuar a análise dos HDs, a PF duplicou os 4 HDs identificados na primeira entrega, usando o equipamento forense Tableau Forensic Imager na modalidade disco para disco, gastando cerca de 23 horas por HD, em 07/11/2017.

Disco	Tempo
Seagate/SRD0NF2/NA8EWZQH	23:16
Seagate/SRD0NF2/NA8EWZKR	23:21
Seagate/SRD0NF2/NA8F1NAJ	23:18
Seagate/SRD0NF2/NA8F7BLS	23:27

Novamente não foi seguindo o procedimento recomendado pelo Ministério Público, sendo que aqui ainda existe um componente agravante:

Esses 4 HDS referenciados no Laudo da PF não são os HDs que vieram originalmente da Suécia, são HDs fornecidos pela própria Odebrecht que gerou uma cópia a partir dos HDs originais e os entregou ao Ministério Público.

Não foi apresentado o Hash nem da cópia original feita pela empresa inglesa FRA, nem o Hash da cópia feita pela empresa Odebrecht.

De fato, na Subseção V.1 do laudo pericial descreve o conteúdo de cada um desses HDs:

> Os peritos verificaram que cada um dos discos possui uma estrutura de pastas e arquivos na qual está contida uma imagem forense, no formato E01, que ocupa a maior parte dos dados armazenados na mídia. De acordo com os arquivos de log, essas imagens forenses foram criadas pelo aplicativo FTK Imager, versão 3.4.2.6, da empresa AccessData, com início em “Fri Mar 17 19:13:54 2017” (Disco 01), “Sat Mar 18 01:47:56 2017” (Disco 02), “Sat Mar 18 01:42:25 2017” (Disco 03) e “Mon Mar 20 10:22:59 2017” (Disco 04).

A tabela 3, elaborada pelos ilustres peritos da PF mostra o conteúdo dos 4 arquivos, cada 1 presente em um HD, com o respectivo Hash, e que seriam os arquivos necessários para serem copiados e analisados. O Hash aqui, é uma mera conferência, uma vez que é material gerado pela própria Odebrecht, mas não atesta a origem do material obtido pela FRA nos computadores da Suécia. Não havendo os hashes originais de Junho de 2016, e sendo a FRA empresa contratada e paga pela Odebrecht, não seria infactível considerar que qualquer informação solicitada à FRA (como por exemplo, conteúdo ou hashes de arquivos) fosse repassada pela mesma para a Odebrecht, e depois encaminhada de volta

pela FRA. Essa dúvida poderia ser resolvida caso a FRA tivesse adotado os procedimentos forenses corretos no momento da clonagem, pois assim a única possibilidade de manipulação dos dados seria desta ter ocorrido anteriormente ao momento da clonagem.

Tabela 3 – Informações sobre os arquivos em formato E01 encontrados nos Discos 01 a 04.

Identificação	Nome do arquivo de imagem	Hashes
Disco 01	\Disk01L\Disk01L.E01	MD5: 435A9F50436040188F74D7C8D28517ED
		SHA1: 0AAF533C45525AC9A471D1DC219D3D3520B9D2F2
Disco 02	\Disk02L\Disk02L.E01	MD5: 72A7ED550AAC583877B29A8F9D2174D8
		SHA1: 08D7279ED957EEE1CBFA6E9CB8561C549069BCCA
Disco 03	\Disk03L\Disk03L.E01	MD5: C7CDBABC68DFC50DFBDBFF3DDEE66CF2
		SHA1: C0D5DA053EF8A6BE9F11DD91C5F56E11BD26A449
Disco 04	\Disk04L\Disk04L.E01	MD5: 372E82DDDE26C7E338829B5ADC4900A3
		SHA1: A04E027308A17DA75F2DFE386A4F31909AAAD56B

O conteúdo de cada um desses arquivos é mostrado no nas tabelas 4, 5, 6 e 7 mostrando claramente que a FRA também não gerou uma imagem forense bit a bit, uma vez que os nomes de arquivos e sua localização, não são típicas do sistema operacional Windows. A FRA usou metodologia própria não padronizada. Alguns arquivos de máquinas virtuais aparentam ter sido clonados corretamente, no entanto não foi apresentado hash para conferência.

Para atestar a integridade dos dados, os peritos da PF trocaram diversos e-mails com a FRA no sentido de obter informações sobre os Hash.

Após intenso trabalho para verificação da integridade, chegou-se a um total de 1.781.609 arquivos, que é diferente do total encontrado pelo MP que obteve 1.781.624. O relatório informa ainda que 607 arquivos não apresentavam integridade.

Constatou-se também ausência de arquivos, o que confirma que a Odebrecht não tratou os arquivos recebidos da FRA com o devido cuidado, eliminando ou alterando vários deles antes de gravar o HD para ser entregue ao MPF.

O próprio MPF acessou o HD simplesmente conectando a uma máquina Windows sem se preocupar em proteger os HDs para escrita, acabando por contaminar ainda mais o material original.

A troca de e-mails entre a PF e a FRA, mostra grave deficiência da FRA com relação a geração de cópia forense, destacada pelos itens seguintes:

- Na folha 36 do Laudo Pericial encontra-se a seguinte observação:

  > Iniciou-se o processo de conferências dos hashes e foi identificado que, nos casos de arquivos de e-mail (extensão EML), o hash do seu conteúdo não era idêntico ao hash encaminhado pela FRA. Posteriormente, foi informado pela FRA que, nesse tipo de arquivo, o hash MD5 havia sido calculado sobre algumas informações do e-mail (assunto, data de envio, remetente, etc), e não sobre o conteúdo total.

- A justificativa da FRA é absolutamente inaceitável e é um erro gravíssimo. Não existe a menor possibilidade em perícia forense, de efetuar cálculo de Hash em arquivos de e-mail apenas com alguns dados, até porque assunto data de envio, remetente, a mensagem estão todos em um único arquivo.
- A PF sugeriu ferramentas de cálculo de Hash para a FRA, que quando enviou o resultado, estava incorreto e truncado, o que mostra a incapacidade da FRA de calcular Hashes de arquivo por arquivo.
- Posteriormente a PF teve que orientar a FRA como efetuar o procedimento.
- É inadmissível que uma empresa especialista em metodologia forense ignore a importância do Hash, que representa o DNA dos arquivos. Não consta em nenhum documento o Hash do HD ou das imagens.

Pela relação entre FRA, Odebrecht ambos intermediando com a PF na tentativa de obtenção de integridade dos arquivos, todo material apresentado não pode ser considerado para análise pericial forense com sendo material integro.

O número de 607 erros em 1.781.609 é **extremamente significativo.** Não existe o conceito de margem aceitável de não conformidades na análise forense. O número correto é sempre ZERO, caso contrário não há como verificar nem a consistência nem a autenticidade dos dados.

A única forma de confiar na integridade desses Hashes seria se a FRA tivesse enviado a relação de Hashes na data da clonagem, como é feito obrigatoriamente em

procedimentos de Busca e Apreensão, por exemplo (pelo Oficial de Justiça), o que não ocorreu.

O material obtido nessa primeira entrega, deve ser considerado imprestável do ponto de vista da perícia forense.

5. Análise da Segunda Entrega

Segundo informações da Odebrecht, os dados provenientes da Suíça foram gerados pelo Ministério Público da Suíça, que os entregou ao escritório Crochet & Cristiano Avocats (patronos da empresa Draftsystem), que os entregou ao escritório suíço de advocacia Schellenberg Wittmer Ltd, e que em 05/2017 os entregou à Odebrecht. São dados referentes aos sistemas informáticos “Drousys” e “MyWebDay B”.

A carta relacionada na folha 25, informa que o procurador federal, Stefan Lenz, enviou carta datada de 27/10/2016, encaminhando mídia com relatórios em PDF, extraídos de My Web Day. Também informa sobre carta do procurador federal Lienhard Ochsner, de 22/03/2017 encaminhando 3 HDs com dados extraídos dos servidores apreendidos localizados no Data Center SafeHost e Interoute e outros dispositivos.
A partir desses dados, a Odebrecht gerou 5 HDs (número bem maior do que os dados vindo da Suiça) e entregou ao MPF/PGR/PR em 08/08/2017. Em 15/08/2017, o MPF/PGR/PR entregou os HDs ao SPPEA/PGR.

Não há nenhuma descrição de metodologia que foi utilizada para a obtenção dessas cópias e nem a geração de Hash.

Se o procurador da Suiça, Stefan Lenz, copiou relatórios em PDF extraídos do My Web Day, é de se deduzir que tiveram acesso ao sistema com a colaboração de pessoa não identificada.

Em nenhum momento foi explicado ou questionado o procedimento de aquisição de quaisquer dos dados constantes da Segunda Entrega, incluindo as imagens de Hds, as coleções de PDFs, e os dados de MIG (celulares, pendrives, notebooks) que não são sequer mencionados nos laudos periciais.

Para efetuar a análise dos HDs, a PF duplicou os 4 HDs identificados na segunda entrega, usando o equipamento forense Tableau Forensic Imager na modalidade disco para disco, gastando cerca de 23 horas por HD, em 07/11/2017.

Disco	Tempo
Seagate/SRD0NF2/NA8EYJ1F	23:22
Seagate/SRD0NF2/NA8F7BLR	23:13
Seagate/SRD0NF2/NA8FDPH9	23:18
Seagate/SRD0NF2/NA8FLDS9	23:27
Seagate/SRD0NF1/NA8CQ6LT	05:04

Como a Odebrecht não forneceu Hash dos HDs gerados pelas autoridades suíças, torna-se impossível saber se as imagens fornecidas se tratam das mesmas informações contidas no original.

Quanto ao conteúdo dos HDs, listados na Tabela 15 do Laudo Pericial (folha 66), observa-se a existência do Hash, que na prática não faz diferença, uma vez que os 4 arquivos foram criados nas dependências da Odebrecht sem que se saiba se representam fielmente os dados que foram enviados pela Suíça, meses antes.

Tabela 15 – Informações sobre os arquivos em formato E01 encontrados nos Discos 05 a 08.

Identificação	Nome do arquivo	HASH
Disco 05	\External HDD 1-1 (1)\External HDD 1-1 (1).E01	MD5: 0F1592EAC0C0E04A0B3A0D941D25CA83
		SHA1: 3DF06177AC70859AFD373B1F96B5546FCDCBE8B1
Disco 06	\Externall HDD 1-1 (2)\External HDD 1-1 (2).E01	MD5: 82FDF3B30625512E4BE43F1C1FD24BDD
		SHA1: DCE997A58721C12BCCE245607D496986F35D3C08
Disco 07	\External HDD 1-2\External HDD 1-2.E01	MD5: DB0864FF934A1BB86A3B29A0803045F6
		SHA1: F7AEAF526D1CDB090370B44DB8053383B0A08DC6
Disco 08	\External HDD 2-1\External HDD 2-1.E01	MD5: 4F80482D5B6FA5B1F9BF52B5059BE0A3
		SHA1: 093D981196DC77C0FB9003C47E62EAEDBAFB4D8C

O trecho do Laudo na folha 68 abaixo, constata a integridade do arquivo gerado na Odebrecht, mas não garante que são os arquivos que vieram da Suíça.

> Em relação aos Discos 05 a 08, inicialmente os hashes embutidos nos próprios arquivos de imagem forense e aqueles localizados nos respectivos

> arquivos de log foram conferidos com o conteúdo dos arquivos de imagem forenses descritas na Tabela 15. Após o procedimento de verificação, foi constatado que o conteúdo dos arquivos recebidos para exame corresponde àqueles que foram criados pela equipe de TI da Odebrecht

Na folha 68 vemos os ilustres peritos concluíram corretamente que a imagem corrompida "\00-DATA\Evidence_Container_SafeHost_SA\DraftSystemInterouteUSB-HD-2.5TB_04.04.2016" presente no Disco 5, já estava corrompida.

> Deve-se acrescentar que o arquivo de imagem forense que contém todas as evidências do Disco 05 ("External HDD 1-1 (1).E01"), apresentado na Tabela 15, encontra-se íntegro. Isso significa que quando a imagem forense gerada pela Odebrecht foi criada, a imagem forense "DraftSystemExtUSBESXi1.E01" já se encontrava danificada.

Importante ressaltar que esse arquivo de imagem foi gerado em 05/04/2016 e que as mídias foram encaminhadas em 27/10/2016, portanto a imagem teria sido gerada mais de 6 meses antes do envio do material e não reflete o estado das cópias.

Esse lapso de tempo causa estranheza e precisaria ser melhor esclarecido, ainda mais em se tratando de um arquivo que leva o nome da empresa que criou o sistema. Do ponto de vista forense, esse é um indício de que este arquivo tenha sido corrompido propositadamente.

Na folha 70 encontra-se o seguinte trecho:

> Para analisar a integridade dos dados recebidos, foi solicitada, à empresa Odebrecht, que fornecesse uma listagem de arquivos com os respectivos hashes. Em resposta, foi recebido um arquivo contendo uma lista de arquivos e os hashes correspondentes, gerados a partir dos arquivos em posse do escritório de advocacia contratado pela Odebrecht na Suíça.

Como se sabe que os hashes gerados vieram a partir dos arquivos em posse do escritório de advocacia contratado pela Odebrecht na Suíça? Não poderiam ter vindo da própria Odebrecht e não da Suíça? Porque logo de início já não vieram esses Hashes?

Em seguida observa-se que a PF comparou corretamente os hashes da listagem que veio:

> Essa listagem foi comparada com os arquivos presentes nos Discos 05 a 08, tendo sido verificado que os arquivos presentes na lista de hashes encontram-se armazenados nesses discos e com hashes idênticos, indicando que não houve qualquer alteração no conteúdo destes arquivos até o momento dos exames.

Não há nenhuma comprovação de não violação, se quem forneceu os hashes foi a própria Odebrecht. Essa lista de hashes deveria ter sido fornecida pelas autoridades Suiças.

No entanto, uma série de não conformidades foram verificadas pela perícia. Arquivos presentes no HD e não presentes na lista, arquivo que está na lista mas não está no HD, vários arquivos que o Hash não corresponde.

A Tabela 21, na folha 72, contém uma quantidade significativa de arquivos inconsistentes.

A perícia ainda identificou que os HDs foram colocados indevidamente em um computador sem a devida proteção de escrita, causando a contaminação dos mesmos.

Destaca-se também, à folha 81 que:

> Após análise dos arquivos/pastas apresentados na Tabela 22, os peritos verificaram a existência de arquivos/pastas com datas de modificação imediatamente anteriores, (em destaque na Tabela 22) às datas de criação dos arquivos de imagem forense pela empresa Odebrecht. A existência desses arquivos indica que, antes da criação dos arquivos de imagem forense, houve a conexão dos discos contendo as evidências encaminhadas pelo escritório de advocacia contratado pela Odebrecht na Suíça em uma porta USB sem que houvesse o bloqueio de escrita sobre as referidas mídias.

Este é um forte indício de que os HDs passaram por uma “inspeção” antes de serem entregues ao MPF.

Do ponto de vista da Análise Pericial Forense, não se pode considerar esses HDs como válidos. Não se pode admitir que não haja 100% de correspondências com os respectivos hashes até porque os arquivos faltantes ou modificados poderiam conter exatamente a informação que se deseja buscar em resposta aos quesitos.

Os HDs possuem tipicamente milhões de arquivos, mas normalmente os que interessam para uma perícia forense e que representam evidências concretas, não chega a 100 arquivos.

O material obtido nessa segunda entrega, deve ser considerado imprestável do ponto de vista da perícia forense.

6. Análise da Terceira Entrega

A terceira entrega é composta por 2 HDs e 1 pendrive entregues pelas autoridades suíças, por meio do Acordo de Cooperação Jurídica Internacional em Matéria Penal Brasil/Suíça, intermediado pelo Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional – DRCI do Ministério da Justiça.

Por se tratar da mesma fonte da 2ª entrega, esses dados deveriam ser os mesmos já fornecidos. A diferença é que estes foram entregues diretamente ao MPF.

Não houve aqui também a verificação dos hashes? Não há clareza sobre quem gerou o material, que metodologia foi usada e quando foi efetuada.

7. Análise da Quarta Entrega

A quarta entrega se refere a um único pen-drive, enviado pela FRA cadastrado como evidência “00051547”, e que não estava presente nos HDs da primeira entrega.

O fato por si só demonstra o despreparo da FRA em lidar com informação forense e coloca em dúvida a lisura de todo processo.

8. Da Análise do Material Recebido

Embora o material recebido pela PF não possa ser considerado íntegro e autêntico, foram efetuadas análises solicitadas, como se estivesse íntegro.

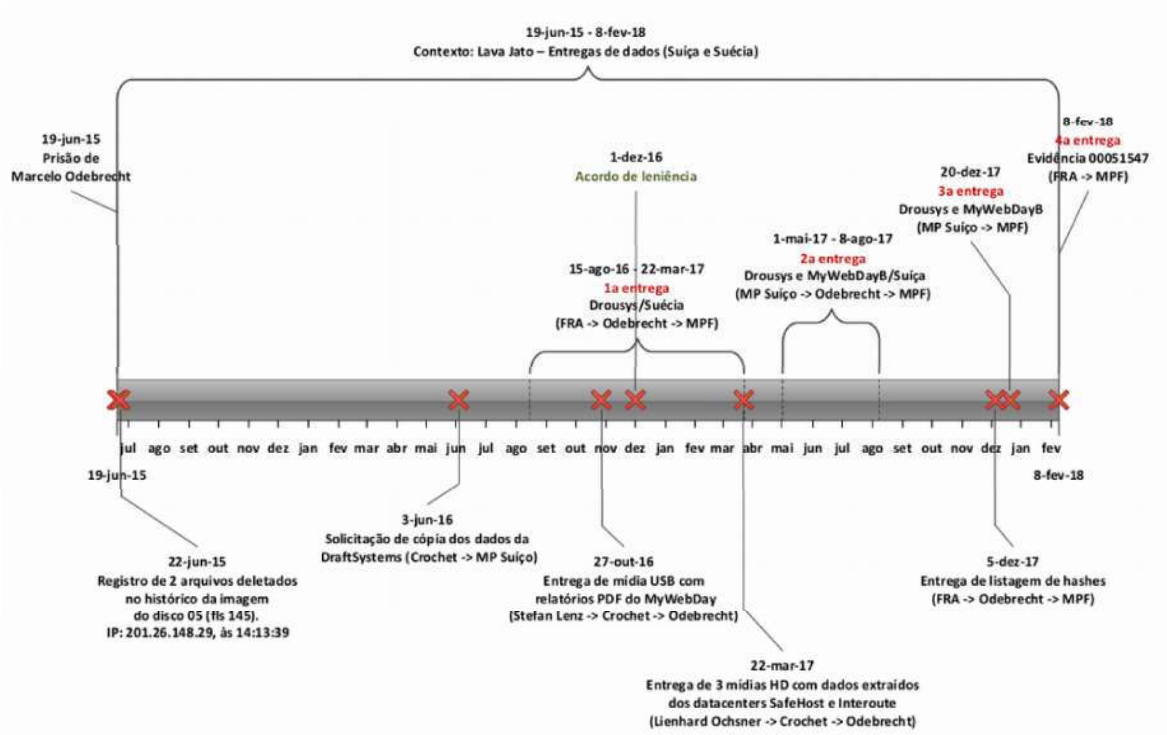
Na folha 122 do laudo, os peritos colocam importante informação:

> É importante destacar que, até o presente momento, não foi possível examinar o ambiente de produção (ambiente real utilizado pelos usuários no dia a dia) do MyWebDay, conforme descrito na Subseção V.14 (página 300). No entanto, os artefatos resultantes da utilização do sistema por usuários (relatórios, consultas), associados a outros elementos como, por exemplo, o ambiente de

desenvolvimento do MyWebDay B, fornecem informações úteis para esclarecer alguns questionamentos, como será demonstrado neste laudo.

Só existe uma razão para que 7 peritos criminais federais, com altíssimo conhecimento técnico, não tivessem conseguido examinar o ambiente de produção. As cópias recebidas dos HDs estavam inconsistentes impedindo que o sistema fosse acessado.

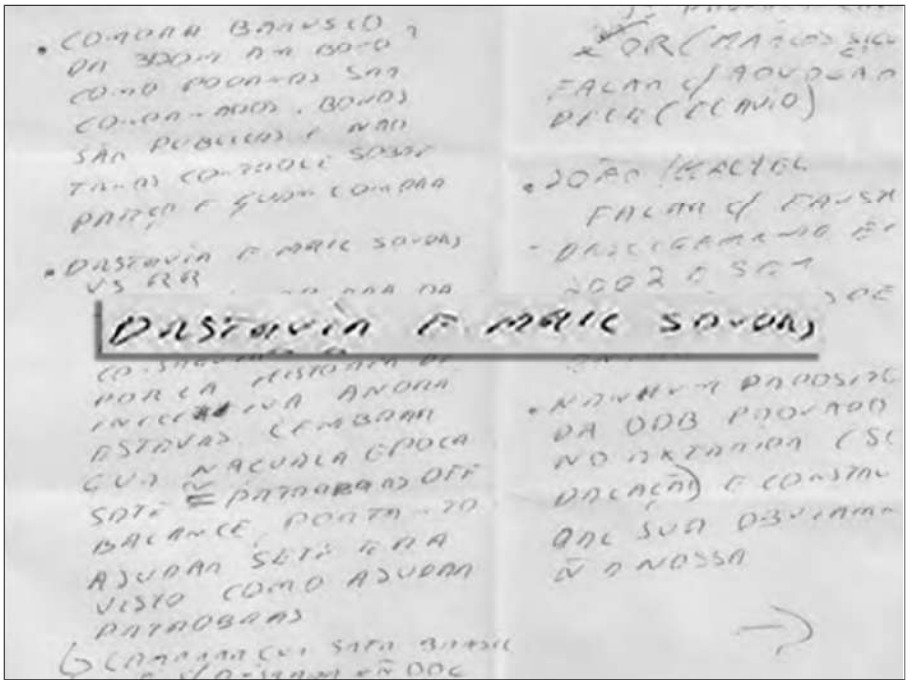
9. Cadeia de Custódia



Os ilustres PFCs, fizeram excelente identificação reportada na folha 301:

> A análise dos históricos de comandos revelou ainda que 3 dessas máquinas virtuais tiveram o conteúdo de seus arquivos deliberadamente "destruídos" através do comando "shred", cuja principal funcionalidade é sobrescrever arquivos com dados aleatórios, de modo a destruir o conteúdo dos arquivos, com objetivo de impedir a leitura dos dados previamente existentes ou recuperação por meio de ferramentas forenses.

Esse fato ocorreu apenas 3 dias após a detenção de Marcelo Odebrecht. Segundo noticiado pela Globo, Marcelo deu ordens explícitas para que arquivos fossem eliminados na mesma data identificada pelos peritos.



Fonte: http://g1.globo.com/pr/parana/noticia/2015/06/destruir-email-sondas-diz-bilhete-de-marcelo-odebrecht-para-advogados.html

> *"...Na carceragem, Marcelo entregou o bilhete a agentes para que ele fosse enviado a seus advogados na segunda-feira (22). Os policiais, que examinam todas as correspondências por medida de segurança, viram a frase sobre o e-mail e decidiram tirar uma cópia da mensagem escrita pelo presidente da Odebrecht..."*
>
> (trecho extraido da reportagem citada)

10. Conclusão

A quantidade de inconsistências encontrada nos HDs periciados pelos PCFs, não permite concluir que o que se encontrou nesse material, possa ser utilizado como fonte fidedigna de informação.

O número de 607 erros em 1.781.609 (na primeira entrega) é **extremamente significativo.** Não existe o conceito de margem aceitável de não conformidades na análise forense. O número correto é sempre ZERO, caso contrário não há como verificar nem a consistência nem a autenticidade dos dados.

O material obtido nas quatro entregas, deve ser considerado imprestável do ponto de vista da perícia forense.

A perícia não conseguiu acessar a base de dados de produção do sistema My Web Day, o que indica que as cópias dos HDs que chegaram ao MPF, vindas da Odebrecht, ou foram alteradas antes da entrega ou foram clonadas de forma inadequada na Suíça e na Suécia, não trazendo os dados completos.

Há evidências de que os sistemas Drousys e My Web Day tenham sido alterados e preparados para que quem fosse examiná-los encontrasse somente aquilo que se desejava encontrar.

Todas as empresas que estiveram envolvidas, de alguma forma, com a obtenção de dados, envio e remessa entre países são ligadas à Odebrecht, na condição de contratados da empresa, e assim muito provavelmente recebendo remuneração pelos serviços prestados..

- Draftsystem, desenvolvedora do Drousys;
- Crochet & Cristiano Avocats (Patronos da empresa Draftsystem na Suiça);
- Schellenberg Wittmer Ltd (Patronos da Odebrecht na Suiça);
- Quinn Emanuel Urquhart & Sullivan (Patronos da Odebrecht nos Estados Unidos);

- FRA (Forensic Risk Alliance) contratada pela Quinn Emanuel Urquhart & Sullivan para gravar os dados da Suécia;

Os dados foram entregues para a Odebrecht no Brasil que após prepará-los os entregou ao MPF.

Os PCFs detectaram que houve manipulação dos dados. Também identificaram volumes criptografados com Truecrypt que poderiam revelar informações importantes, mas ao solicitarem a senha para a Odebrecht foram informados que a empresa esqueceu a senha.

São Paulo, 16 de março de 2018

Paulo Cesar Breim

John D Rowell

Natalia Moniwa