

LAUDO TÉCNICO

1 - Premissas

O abaixo assinado Lorenzo Parodi, perito em fraudes e falsificações, inscrito no rol dos peritos da Justiça Federal, do TJSP e de diversos outros Tribunais Estaduais, e atuante nestes órgãos na qualidade de Perito Judicial nas áreas acima, autor do livro “Manual das Fraudes” (1ª e 2ª edição, 2005 e 2008) e do livro “Falsificação de Documentos em Processos Eletrônicos” (2018), todos pela Editora Brasport, além de numerosas matérias e artigos de cunho acadêmico publicados, entre outros, pelos reconhecidos portais *Conjur*, *Migalhas*, *Administradores* e *Monitor das Fraudes*, foi contratado, através da empresa IBRACAF - Serviços de Prevenção e Combate a Fraudes Ltda., pela [REDACTED], representada por sua advogada [REDACTED] para analisar um conjunto de documentos, questões técnicas e afirmações existentes no processo penal n. 0073766-87.2018.4.02.5101 perante a Justiça Federal, Seção Judiciária do Rio de Janeiro (e, em parte, no inquérito n. 0060662-28.2018.4.02.5101 que o gerou), com o intuito geral, entre outros, de verificar sua autenticidade, consistência e validade como provas.

2 - Escopo e Quesitos

Os documentos objeto de análise são todos em formato digital (ou eletrônico), juntados aos autos como arquivos no formato PDF e alegadamente fornecidos por colaboradores ao Ministério Público Federal na forma de arquivos eletrônicos salvos em um HD (Hard Disk).

Se trata dos seguintes arquivos eletrônicos:

- a) Arquivo composto por 638 páginas, denominado “[REDACTED] (Cabral) - BankDrop.pdf”, com dimensão de 95.286.911 Bytes e HashCode SHA3-256 (a0b84b56ca44006eb2c0d13365c04494fe57cb45e4a1046880a1f080bc4a54e1), doravante indicado como “Documento A”.
- b) Arquivo composto por 41 páginas, denominado “Extrato conta Cabral.pdf”, com dimensão de 256.974 Bytes e HashCode SHA3-256 (4b803de644b85dd7f9a8a6abe3d7a5b794523f3913587e4672bc8decbe243a45), doravante indicado como “Documento B”.

Adicionalmente, para responder alguns dos quesitos, foi analisado o já mencionado HD (Hard Disk da marca Western Digital com capacidade de 1TB), que foi fornecido, em tese sendo cópia idêntica àquela do HD presente nos autos (clone), pela serventia da Vara competente, em data 12/07/2018.

O HashCode SHA-256 do “drive” integral, que identifica de forma unívoca tal HD, foi calculado como sendo o seguinte (entre parênteses):

(30344e62875d4c2b5a59824c7be8a60d5ac132ee165222c02832e8ef291d9b8b)

Os **quesitos** postos, relativamente aos documentos acima mencionados assim como juntados aos autos do processo em foco, ao HD acima identificado e a outras questões relacionadas ao citado processo, são os seguintes:

- 1) A partir da análise do HD apresentado como suporte probatório pelo MPF e disponibilizado à defesa, diga o perito se todas as imagens utilizadas na denúncia e no despacho que a recebeu, que culminou com a ação penal, em relação a [REDACTED], estão armazenadas no referido HD?
- 2) Que tipos de arquivos são aqueles presentes no referido HD?
- 3) Analisando as imagens presentes no Documento A, que se referem ao suposto sistema “Bankdrop” é possível afirmar que as mesmas tenham sido extraídas de um software/sistema ou se trata apenas de arquivos eletrônicos contendo imagens que podem ter sido geradas de qualquer maneira?
- 4) Analisando o HD disponibilizado à defesa, é possível dizer se há nele algum software ou sistema, ou se o mesmo contém somente documentos e imagens?
- 5) Analisando o Documento A, que contém imagens do suposto sistema Bankdrop, é possível afirmar que seria software de banco de dados?
- 6) Em caso positivo, diga o perito se o referido banco de dados está armazenado no HD?
- 7) Analisando o Documento A, que contém imagens do suposto sistema Bankdrop, e outros documentos presentes no HD, é possível afirmar que existam duas versões do referido “sistema”?
- 8) Com base nos elementos disponíveis nos autos é possível afirmar que duas versões diferentes dos supostos softwares, eventualmente usados para originar as imagens reproduzidas nos documentos acima, teriam o mesmo funcionamento e utilizariam a mesma base de dados?
- 9) Analisando os arquivos Documento A e Documento B, disponibilizados no HD é possível saber qual sua fonte?
- 10) Analisando os arquivos Documento A e Documento B apresentados no HD, sem que se tenha acesso à sua fonte é possível assegurar que as informações neles indicadas sejam autênticas?
- 11) Analisando os Documentos A e B apresentados no HD, e as imagens neles contidas, é possível verificar indícios ou evidências de edição ou adulteração?
- 12) Em caso positivo, de que natureza quais seriam as alterações?
- 13) Os Documentos A e B, no estado em que se encontram, são aptos a comprovar o teor das informações neles contidas?
- 14) Diga o perito a respeito da existência, consistência, preservação e efetividade da cadeia de custódia dos documentos em foco, presentes nos autos?
- 15) Diga o perito se é possível afirmar que os documentos em foco são autênticos e não foram objeto de eventuais adulterações ou edições?
- 16) Após análise dos documentos e dos autos do processo disponibilizados, diga o perito se tais documento constituem provas válidas e admissíveis em seu estado atual?

17) Há, entre os documentos presentes no HD, algum que relacione o apelido “CABRAL” ao nome da [REDACTED]?

Para executar os trabalhos foram utilizadas diferentes ferramentas de análise, entre as quais mencionamos os softwares PDF-Analyzer 5.0, AutoMetadata (Evermap), Ghir0 0.2.1 (ELA), OSFClone 1.3, WinDirStat 1.1.2 e Autopsy 4.7.

O presente trabalho diz respeito exclusivamente aos documentos, HDs e questões acima identificados, não sendo aplicável a outros documentos ou questões eventualmente existentes no mesmo processo, similares ou não.

3 - Análises e Respostas

Antes de responder os quesitos postos, é oportuno definir, de forma mais exata e pontual, alguns termos mencionados nos quesitos e nas respostas abaixo, e importantes para o melhor entendimento deste trabalho.

Prova, em sentido jurídico, é todo e qualquer elemento material legítimo e lícito que, após sua validação, sirva para demonstrar, comprovar ou esclarecer o que foi alegado pelas partes, especialmente circunstâncias fáticas, com intuito de formar e embasar o convencimento do julgador.

Indício. De acordo com o Art. 239 CPP, “*Considera-se **indício** a circunstância conhecida e **provada**, que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra ou outras circunstâncias.*” [grifos nossos].

Vestígio (palavra encontrada nos Artigos 158 e 564 CPP) é qualquer marca, objeto, elemento ou sinal sensível que possa ter relação com o fato investigado e que, após análise pericial que o enquadre no caso, em decorrência da confirmação de sua autenticidade e da relação inquestionável com o fato e com as pessoas envolvidas, passa a ser considerado como indício ou prova.

Sistema (informático) é um conjunto de software (programas), hardware (computadores) e dados, que tem por objetivo realizar determinadas operações (suas funções) que podem ser elaborações, comunicações, visualizações, impressões ou simples armazenamentos de informações, normalmente tendo como base sempre os dados do sistema (que podem ser digitados, transmitidos, importados, armazenados, criados etc.).

Documento é qualquer registro de informações, independentemente do formato ou suporte utilizado para registrá-las (pode ser suporte cartáceo, eletrônico etc.). Por óbvio, o documento pode ser autêntico ou não, verídico ou não etc. Como diz o ditado: “o papel aceita tudo”.

Por essa razão, para que um documento eletrônico possa ser considerado como prova válida é necessário que seja previamente verificada sua autenticidade (Art. 439 CPC e Art. 158 CPP).

Corpo de delito é o conjunto dos vestígios supostamente resultantes da prática criminosa ou a ela relacionados.

Após detida análise de todo o material fornecido pela contratante, que inclui os documentos acima mencionados (Documento A e Documento B), o referido HD e parte das principais peças presentes nos autos, considero corretas e fundamentadas as seguintes respostas aos quesitos postos:

- **Resposta ao Quesito 1.**

Primeiramente, através de apropriada ferramenta forense, foi clonado o HD original fornecido pela serventia da Vara, de forma a preservar tal mídia como já identificada no ponto anterior através de hashcode SHA-256. Os trabalhos foram realizados no clone assim obtido.

O conteúdo original do HD é formado por 28 pastas, mais um arquivo separado chamado “.dropbox.device” (além das pastas “System Volume Information” e “Recycle.Bin”, administradas pelo sistema), conforme Fig. 01.

[041201e7f74ce8bf581c8642ec]	<DIR>	11/07/2018 12:48
[Anexo 1 - Trajetória profissional dos colaboradores]	<DIR>	11/07/2018 13:08
[Anexo 10 - Operações de Diego Candolo]	<DIR>	11/07/2018 13:09
[Anexo 11 - Doleiro Carlos Garibe]	<DIR>	11/07/2018 13:09
[Anexo 12 -Doleiro Paulo Arruda]	<DIR>	11/07/2018 13:09
[Anexo 15 - Doleiro Henrique Chueke (Kaluf)]	<DIR>	11/07/2018 13:09
[Anexo 16 - Doleiro Davies]	<DIR>	11/07/2018 13:09
[Anexo 17 - Flavio Dib]	<DIR>	11/07/2018 13:09
[Anexo 18 - Operações Marco Antonio Cursini (Massita)]	<DIR>	11/07/2018 13:15
[Anexo 19 - Operações Irmãos Rezinski (Pedra)]	<DIR>	11/07/2018 13:15
[Anexo 2 - Logística das Operações (Trans-Expert)]	<DIR>	11/07/2018 13:09
[Anexo 21 - Cliente Banco Bozano Simonsen]	<DIR>	11/07/2018 12:45
[Anexo 24 - Yasha Mughrabi (Monza)]	<DIR>	11/07/2018 12:49
[Anexo 26 - Doleiro Claudio Freitas (Papaia)]	<DIR>	11/07/2018 12:50
[Anexo 27 - Sergio Mizrahy]	<DIR>	11/07/2018 12:51
[Anexo 29 - Richard Otterloo (XOU)]	<DIR>	11/07/2018 12:59
[Anexo 30 -Operações com Alberto (Leoncio)]	<DIR>	11/07/2018 13:00
[Anexo 31 - Operações de Nei e Rene]	<DIR>	11/07/2018 13:00
[Anexo 32 -Doleiro Henrique (Fofinho)]	<DIR>	11/07/2018 13:01
[Anexo 33 - Paulo Cordeiro (Asado)]	<DIR>	11/07/2018 13:01
[Anexo 34 - Lino Mazza]	<DIR>	11/07/2018 13:01
[Anexo 38 - Doleiro Jubra]	<DIR>	11/07/2018 13:01
[Anexo 39 - Doleiros Saliba e Camilo]	<DIR>	11/07/2018 13:01
[Anexo 40 - Claudine Spiero (Cabral)]	<DIR>	11/07/2018 13:07
[Anexo 41 - Dario Messer]	<DIR>	11/07/2018 13:08
[Anexo 45 - Chines]	<DIR>	11/07/2018 13:08
[Anexo 56 - Rony Hamoui (Jacinto)]	<DIR>	11/07/2018 13:08
[Anexo 9 - Familia Matalon]	<DIR>	11/07/2018 13:09
[System Volume Information]	<DIR>	12/07/2018 08:01
.dropbox	device	56 12/07/2018 08:01

Figura 01

Fundamental observar que as pastas têm como data de criação o dia 11/07/2018 o que indica que o HD fornecido pela serventia da Vara, não foi clonado a partir do original, ou seja, no fornecimento da cópia do HD à defesa, não foram adotados os normais e indispensáveis procedimentos de análise forense para preservar a integridade e garantir a segurança e idoneidade das mídias que deveriam conter vestígios ou provas.

Na prática foram simplesmente copiadas as pastas contidas no HD original (sem qualquer cuidado quanto a sua preservação), e não foram reproduzidas as demais características daquela mídia, eliminando portanto a possibilidade de verificar a existência de outros arquivos cancelados assim como de informações adicionais sobre a origem do HD original e de seu conteúdo (por exemplo as datas das pastas ou de alguns arquivos).

Adicionalmente, utilizando esta modalidade insegura, não se pode excluir que algum arquivo (num universo de mais de 15mil arquivos) tenha sido acidentalmente omitido ou alterado na cópia.

De toda forma o HD em questão foi analisado detalhadamente com o uso de um respeitado software forense (Autopsy 4.7), e resultou (como previsível pelas razões acima) que não há arquivos ocultos válidos nem arquivos cancelados recuperáveis.

Por essa razão, serão considerados, para fins da resposta ao presente quesito, somente os arquivos encontrados e evidentes nas diversas pastas do HD (inclusive aqueles obtidos após descompactar os 90 arquivos compactados nos formatos ZIP e RAR), conforme resumidamente listados na resposta ao Quesito 2.

Com reserva de erro, considerado o enorme número de arquivos presentes no HD, os diversos milhares de páginas dos documentos e peças que compõem o processo (denúncias, autuações, decretos, incidentes etc.) e, sobretudo, a falta de uma organização e referência correspondente ao uso de tais arquivos nas peças mencionadas (onde imagens são usadas sem informar de onde foram extraídas ou obtidas), relativamente a [REDACTED] e ao codinome "Cabral", que foi a ela atribuído pelos colaboradores, não foram encontrados no mencionado HD os arquivos que deveriam conter as seguinte imagens:

1. Imagem reproduzida às fls. 275 da denúncia do MPF em data 08/06/2018.
2. Imagem reproduzida às fls. 704 do termo de atuação da 7ª Vara Federal Criminal do Rio de Janeiro, em data 16/04/2018.
3. Imagem reproduzida às fls. 705 do termo de atuação da 7ª Vara Federal Criminal do Rio de Janeiro, em data 16/04/2018.

• Resposta ao Quesito 2.

Conforme informado na resposta ao Quesito 1, no HD fornecido pela serventia da 7ª Vara Federal Criminal do Rio de Janeiro, foram encontradas 28 pastas, dentro das quais resultaram presentes um total de 15.653 arquivos, divididos em 853 subpastas, de acordo com o resumo abaixo (Fig. 02):




















Extension	Description	Bytes	% By...	Files
 .pdf	Adobe Acrobat Document	3,5 GB	43,7%	5.983
 .jpg	JPEG image	2,8 GB	34,9%	4.517
 .docx	Microsoft Word Document	1,5 GB	18,9%	1.355
 .zip	Compressed (zipped) Folder	86,3 MB	1,1%	77
 .jpeg	JPEG image	44,4 MB	0,5%	57
 .rar	RAR File	30,6 MB	0,4%	13
 .bmp	Bitmap image	11,4 MB	0,1%	1
 .doc	Microsoft Word 97 - 2003 Document	6,1 MB	0,1%	34
 .xls	Microsoft Excel 97-2003 Worksheet	4,5 MB	0,1%	37
 .png	PNG image	4,1 MB	0,1%	43
 .xlsx	Microsoft Excel Worksheet	2,7 MB	0,0%	19
 .db	Data Base File	2,4 MB	0,0%	30
 .txt	Text Document	2,3 MB	0,0%	3.467
 .tif	TIFF image	908,3 KB	0,0%	5
 .odt	Text OpenDocument	882,2 KB	0,0%	1
 .911 skiway monza zorro	File	94,1 KB	0,0%	2
 .html	Chrome HTML Document	66,9 KB	0,0%	10
 .ini	Configuration settings	129 Bytes	0,0%	1
 .device	DEVICE File	56 Bytes	0,0%	1

Figura 02

Importante detalhar algumas características dos principais tipos de arquivos presentes neste HD, de acordo com sua extensão (ou “*extension*” em inglês):

- PDF - são documentos (Acrobat) que podem conter texto ou imagens
- JPG, PNG, BMP, TIF - são imagens
- DOC, DOCX, ODT - são textos ou documentos (MS Word ou Libreoffice)
- XLS, XLSX - são planilhas (MS Excel)
- TXT - são textos simples
- ZIP, RAR – são pastas ou arquivos variados compactados
- HTML - são páginas de documentos em formato web (internet)

Importante, também, explicar que todos os 30 arquivos com extensão “DB”, indicados como “*data base file*”, são de fato arquivos com o mesmo nome “*thumb.db*” em pastas diferentes.

Os arquivos denominados “*thumb.db*” são criados automaticamente pelo sistema e contém miniaturas das imagens presentes em determinada pasta, para facilitar sua visualização e listagem. NÃO são bases de dados do tipo discutido neste trabalho, como se poderia pensar pelo nome.

Oportuno observar que, dentre os arquivos acima, se encontram 90 arquivos compactados (tipos ZIP e RAR) os quais, uma vez descompactados, resultaram em um outro conjunto de 692 arquivos adicionais (com 3 diferentes subpastas) dos seguintes tipos (Fig. 03):






Extension	Description	> Bytes	% Bytes	Files
 .jpg	JPEG image	105,7 MB	69,4%	423
 .pdf	Adobe Acrobat Document	46,5 MB	30,6%	250
 .html	Chrome HTML Document	66,9 KB	0,0%	10
 .doc	Microsoft Word 97 - 2003 Document	54,5 KB	0,0%	2
 .	Local Disk	1,8 KB	0,0%	7

Figura 03

- **Resposta ao Quesito 3.**

Oportuno mencionar, neste ponto, que, conforme melhor detalhado na resposta ao Quesito 15, somente o Documento A contém imagens. O Documento B, por sua vez, é formado exclusivamente por texto formatado de forma que possa parecer que se trate de imagens de telas capturadas, quando na realidade se trata somente de texto.

Apesar de sua aparência sugerir que as imagens presentes no Documento A sejam produto da captura de telas de algum software/programa, não há como ter certeza disso com base somente em tais imagens.

De fato a origem das imagens presentes no Documento A é desconhecida, não têm nenhum tipo de informação adicional em seu interior, os dados dos arquivos EXIF internos (onde, no caso de imagens JPG, podem estar armazenadas informações sobre a origem da imagem) são vazios, o mesmo se pode dizer em relação às demais imagens em formato PNG, BMP e TIF.

Por tudo quanto acima as imagens em questão somente podem ser consideradas como imagens sem qualquer elemento fático que permita confirmar que se refiram a algum software ou que tenham sido capturadas ou produzidas pelo suposto software que aparentam reproduzir.

Pelos elementos disponíveis, é perfeitamente possível que tais imagens tenham sido, simplesmente, criadas, ex novo, utilizando programas de gráfica ou através de montagens de diversos tipos.

- **Resposta ao Quesito 4.**

Destarte é oportuno mencionar que um software executável, que tenha portanto capacidade para realizar tarefas, elaborar dados etc., é formado por arquivos que têm normalmente a extensão EXE. Existem algumas outras extensões que podem, adicionalmente, compor softwares executáveis quais DLL, BIN, VB, VBS, VBE, COM, CMD (as principais).

Conforme já indicado anteriormente (ver resposta ao Quesito 2), o HD analisado contém prevalentemente documentos (em formato Acrobat PDF, MS Word, LibreOffice e Texto), imagens (em diversos formatos) e arquivos de tabelas no formato MS Excel.

Não há, no HD em foco, nenhum dos arquivos executáveis (ou parte de softwares executáveis) acima listados, nem qualquer outro conhecido.

Isso significa que não foi encontrado nenhum software executável nem bases de dados (por exemplo em formato MDB ou em algum padrão SQL) que poderiam eventualmente alimentar um tal software.

Também não foram encontrados arquivos de bases de dados que possam ser administradas isoladamente por softwares de gestão de dados, como os arquivos MDB que podem ser administrados pelo software MS Access (parte do pacote Office da Microsoft), ou outros tipos de bases de dados.

• **Resposta ao Quesito 5.**

Conforme já informado anteriormente (ver resposta ao Quesito 3) não é possível sequer afirmar que tais imagens se refiram, de fato, a um software. Menos ainda é possível dizer quais seriam as características de um eventual software, sem poder analisar ele.

Se tal software realmente existir, considerando que as imagens das supostas telas capturadas apresentam listagens de dados, com diversos registros e campos, é bastante provável que o mesmo (como a maioria dos softwares deste tipo) funcione atrelado a algum tipo de base de dados.

Não é possível, porém, informar com certeza quais tipos de elaborações o software poderia realizar sobre os eventuais dados. Pelos botões que aparecem nas imagens (se de fato funcionarem conforme indicados na denominação deles) poderia se imaginar que tal eventual software tenha funções bastante básicas como: “inserir dados”, “modificar dados”, “cancelar dados” e realizar buscas nos dados existente, baseadas em datas e/ou em chaves específicas.

Não foram encontrados indícios que possam fazer pensar a realização de algum tipo de cálculo ou outras elaborações mais complexas.

• **Resposta ao Quesito 6.**

Conforme já informado na resposta ao Quesito 4, não foi encontrado no HD analisado nenhum arquivo que tivesse um formato conhecido de banco de dados, sendo os únicos tipos de arquivos presentes no HD em foco, aqueles já listados anteriormente na resposta ao Quesito 2.

- **Resposta ao Quesito 7.**

Reiterando que não é possível sequer dizer que exista, de fato, um software chamado Bankdrop, pode-se observar que existem no Documento A imagens que reproduzem um suposto software denominado Bankdrop.

Por outro lado, nos autos do processo foram localizadas diversas outras imagens que aparentam representar um software denominado Bankdrop. Neste caso se trata de imagens parecidas, mas não iguais, em todas suas características, àquelas presentes no Documento A.

Por exemplo na denúncia oferecida pelo MPF em 06/06/2018, perante a 7.a Vara Federal Criminal do Rio de Janeiro, se encontram diversas de tais imagens diferentes (ver lista na Fig. 05) do suposto software “Bankdrop”.

Uma, entre outras diferenças, que se observa em todas estas imagens, é o número de versão do suposto software Bankdrop e do computador e conta de usuário no qual ele estaria funcionando (ver Fig. 04).

Foram encontrada 7 versões diferentes do software com ao menos 8 diferentes usuários (deixamos, inclusive, de contar alguns usuários) em 2 diversos computadores (Fig. 05). Isso desconsiderando que o nome “DESKTOP” é muito comum e poderia muito bem ser usado por computadores diferentes.



Figura 04

Com base em quanto acima é razoável supor que, caso o suposto software “Bankdrop” exista realmente, devem existir diversas versões do mesmo, funcionando em diferentes computadores e com diferentes contas de usuário de tais computadores, de acordo, no mínimo, com a tabela abaixo:

Versão	Computador	Usuário	Documento	Página
2.0.50727.8794	DESKTOP	KHADJDF	Doc. A	1
2.0.50727.8825	DESKTOP	9T92F8I	Denuncia	197
2.0.50727.8922	DESKTOP	T24CTLL	Denuncia	231
2.0.50727.5472	RP	70071	Denuncia	347
2.0.50727.8830	DESKTOP	NDI1D1M	Denuncia	504
2.0.50727.8745	RP	021871	Denuncia	558
2.0.50727.8766	RP	30021868	Denuncia	613
2.0.50727.8825	RP	021876	Denuncia	662

Figura 05

O fato que o mesmo software funcione em computadores diferentes e com contas de usuário diferentes, leva a pensar que, muito provavelmente, utilize também bases de dados diferentes e locais em cada computador, pois seria complexo articular uma sincronização de todos estes diversos usuários e computadores, sem considerar que diferentes versões do software poderiam facilmente significar incompatibilidade entre os respectivos dados.

Podem ainda ser mencionadas outras diferenças encontradas em telas presentes em outros documentos que compõem os autos como, por exemplo, aquelas detalhadas na resposta ao Quesito 10 em relação às telas reproduzidas nas páginas 596 e 704 (Figuras 06 e 07) do termo de atuação, emitido em 16/04/2018 pela 07ª Vara Federal Criminal do Rio de Janeiro.

- **Resposta ao Quesito 8.**

Considerando que não há, nos autos, cópias de tais softwares que possam ser analisadas, não é certamente possível afirmar que duas (ou mais) versões de um software tenham as mesmas funcionalidades e utilizem o mesmo formato e tipo de dados (ou de banco de dados).

Menos ainda é possível afirmar que os dados utilizados pelos dois softwares sejam os mesmos, sem ter acesso aos arquivos que contêm tais dados.

Qualquer afirmação diferente, não lastreada numa análise detalhada de tais softwares e dados, por obvio, não passaria de um exercício de adivinhação.

É lógico pensar que, se há versões diferentes de um determinado software, estas versões tenham diferenças (pois se não tivessem, não faria sentido criar versões diferentes).

Tais diferenças podem ser grandes ou pequenas, evidentes ou ocultas, e podem dizer respeito a qualquer um dos muitos aspectos de um software, desde questões meramente estéticas, passando pela implementação de diferentes funções e funcionalidades até o uso de formatos de dados diferentes (que podem, ainda, ser compatíveis ou incompatíveis entre si).

Para saber quais sejam tais diferenças é, obviamente, necessário e imperativo poder analisar detidamente os softwares em questão (em todas suas versões existentes) e seus respectivos dados.

Resta evidente, portanto, à luz das informações e do material presentes nos autos (que não inclui qualquer software, sistema ou base de dados), que é **totalmente descabida e priva de qualquer mínima fundamentação técnica e lógica a eventual afirmação que duas versões diferentes de determinado software tenham o mesmo funcionamento e utilizem os mesmos dados.**

Oportuno frisar, que, caso tal afirmação (quanto à identidade de funcionamento e de dados entre duas versões diferentes de software) pretenda ser utilizada como prova num processo penal, deverá ser previamente verificada e validada através de oportuna perícia oficial, a ser certamente e inevitavelmente realizada nos vestígios constituídos pelas duas (ou mais) versões originais dos supostos softwares em foco e nos relativos dados, comprovando a origem e preservando a necessária cadeia de custódia, conforme inexoravelmente determinado pelo já mencionado Art. 158 CPP.

• Resposta ao Quesito 9.

Destarte seria oportuno definir o que se entende por “fonte”? Se a fonte é o software que os originou, ou a pessoa/usuário que realizou tal operação, ou ainda o computador no qual tal operação foi executada?

Conforme detalhado na resposta ao Quesito 15, os mencionados arquivos são composto da seguinte forma:

- a) Documento A, composto por imagens impressas verticalmente.
- b) Documento B, composto por simples texto formatado apropriadamente.

Seja qual for a definição de “fonte” que se deseja utilizar, não há qualquer elemento que permita individualizar a origem e fonte de tais Documentos, fora o fato que foram criados em datas diferentes (ambas em 2018), por usuários diferentes e provavelmente em computadores diferentes (conforme detalhado na Fig. 05).

A real fonte é totalmente desconhecida e poderia ser tanto um eventual software como aquele que aparece indicado nas imagens, quanto imagens e texto criados e/ou manipulados sob medida para criar tais arquivos.

Neste sentido oportuno observar o arquivo em formato PDF, denominado “*exemplo_falso.pdf*”, anexado a este laudo, onde foi simulado um documento no mesmo idêntico formato do Documento B (recriamos somente as primeiras 4 páginas, para evitar produzir muito volume inutilmente), mas com dados fictícios que indicam um inventado codinome “XXXXXX” no lugar do codinome “CABRAL”.

Tal arquivo foi criado com um banalíssimo editor de texto MS Word, em questão de minutos, somente para mostrar como é fácil criar (ou forjar) um documento de texto e depois imprimi-lo no formato PDF simulando a existência de um software que o teria impresso.

• Resposta ao Quesito 10.

Mesmo admitindo, por mera hipótese, que exista um software chamado “Bankdrop” e que este software tenha um único banco de dados usado por todas suas versões, sincronizado-se continuamente.

Ainda assim não seria possível, à luz dos arquivos e informações presentes no HD em foco, assegurar que as informações contidas no Documento A sejam autênticas e verdadeiras sem realizar um profunda perícia em tal software e dados e comprovar a existência e solidez de uma cadeia de custódia de tal software e dados.

Isso porque, por exemplo, não se poderia excluir que o suposto software tenha sido criado no final de 2017 ou início de 2018 (qualquer jovem programador poderia realizar um tal simples software em pouco tempo e por pouco dinheiro), abastecido com informações e dados falsos, em tudo ou em parte, de interesse de alguém (por exemplo para suportar e dar lastro a uma colaboração premiada que diversamente não seria aceita ou, ainda, para prejudicar desafetos ou por diversas outras razões), e depois tenha sido utilizado para produzir telas com datas fictícias a serem capturadas para integrar o Documento A (em formato PDF).

Para alguns poderá parecer que esta hipótese seja fantasiosa mas, de um ponto de vista fático e objetivo, baseado na análise forense dos arquivos presentes no HD em foco, não há nenhum elemento que permita excluir ou duvidar desta hipótese, que deve, portanto, ser considerada tão potencialmente válida, crível e sólida quanto qualquer outra, inclusive aquela que as telas tenham sido produzidas graficamente, sem a existência de qualquer software subjacente, ou, ainda, aquela proposta pelos colaboradores e pelo MPF.

Neste sentido é oportuno mencionar, por exemplo, a existência nos autos de duas imagens representando telas do suposto sistema Bankdrop, que reportam o mesmo registro com características profundamente diferentes uma da outra.

Tais telas, provavelmente produzidas em momentos diferentes, por usuários diferentes e, caso exista um efetivo software Bankdrop, por versões diferentes deste software, reproduzem informações de uma mesma suposta transação financeira, selecionada pelo usuário (de acordo com o que aparece nas imagens), mas com características bem diferentes uma da outra.

No termo de atuação, emitido em 16/04/2018 pela 7ª Vara Federal Criminal do Rio de Janeiro, pode se observar que na página 596, existe a tela reproduzida na Figura 06 a seguir.

BankDrop v2.0.50727.8794 en DESKTOP-KHADJDF

Favorecido
 Nombre: **HEXA TRADE LINE LTD**
 Direccion: **TRIDENT CHAMBERS WICKHAMS CAY F**
 IBAN # **CH7 008 624 047 091 010 008**
 NoCuenta: **470 910**

Banco Beneficiario
 Nombre: **BANQUE AUDI**
 Direccion: **2 RUE MASSOT C.P. 384 - 1211 GENEVA 12, SWI**
 Estado: **GENEVE**
 País: **SUISSE**
 Swift: **AUDSCHGGXXX**

Banco Intermediario
 Nombre: **JPMORGAN CHASE BANK, N.A.**
 Direccion: **4 NEW YORK PLAZA FLOOR 15**
 Estado: **NEW YORK**
 País: **USA**
 Swift: **CHASUS33XXX**

Datos
 Cliente: **CABRAL** BK **C. KAUFMAN** Fecha **18/07/2014**
 Valor **US\$ 20.720.00** Total **US\$ 250.000.00**
 Motivo: **APLICACAO**

Formato Texto
 Banco: **BANQUE AUDI**
 GENEVE/SUISSE
 Swift: **AUDSCHGGXXX**
 End : **2 RUE MASSOT C.P. 384 - 1211 GENEVA 12, SWITZERLAND**

Seguimiento
 18/07/2014 - CARMEN
 (12:41:32 PM) Cabral: 20720 confirmados hexa (12:42:08 PM) Cabral: falta so 50 (12:48:19 PM) emmacatt2014@gmail.com/39814610: Ok, blz (12:48:39 PM) emmacatt2014@gmail.com/39814610: item como ver que dia chegou ? (12:49:52 PM) Cabral: os 20720? (12:50:40 PM) Cabral:

Ingreso **CARMEN 18/07/2014** Modificado **CARMEN 18/07/2014** **Confirmado CARMEN 18/07/2014**

ID	Confirm	Fecha	Mon	Valor	Total Orden	Cliente	BK	Fav.Cuenta	Fav.Nombre	Favorecido Direccion	Banco
101477	<input checked="" type="checkbox"/>	07/07/2014	US\$	17,000.00	149,000.00	CABRAL	ILLY	461 620	HALSON TRADI...	SWISS TOWER, 16...	BANQUE AUDI
101484	<input checked="" type="checkbox"/>	09/07/2014	US\$	31,800.00	262,000.00	CABRAL	MAURIZIO	356 200	BURGEL ASSOC...	CALLE 53E, URBAN...	BANQUE AUDI
101485	<input checked="" type="checkbox"/>	09/07/2014	US\$	31,800.00	262,000.00	CABRAL	MAURIZIO	356 200	BURGEL ASSOC...	CALLE 53E, URBAN...	BANQUE AUDI
101489	<input checked="" type="checkbox"/>	10/07/2014	US\$	250,000.00	0.00	CABRAL	ILLY	OSA 110 081 640 478...	D AND C FORT...	5TH .G DISTRICT J...	SHENZHEN DEV...
101492	<input checked="" type="checkbox"/>	11/07/2014	US\$	20,720.00	250,000.00	CABRAL	C. KAUFMAN	470 910	HEXA TRADE LI...	TRIDENT CHAMBE...	BANQUE AUDI
101493	<input checked="" type="checkbox"/>	11/07/2014	US\$	129,100.00	200,000.00	CABRAL	VESTRIOGAB	470 910	HEXA TRADE LI...	TRIDENT CHAMBE...	BANQUE AUDI
101494	<input checked="" type="checkbox"/>	11/07/2014	US\$	100,000.00	200,000.00	CABRAL	SEB	470 910	HEXA TRADE LI...	TRIDENT CHAMBE...	BANQUE AUDI
101504	<input checked="" type="checkbox"/>	15/07/2014	US\$	20,000.00	250,000.00	CABRAL	C. KAUFMAN	470 910	HEXA TRADE LI...	TRIDENT CHAMBE...	BANQUE AUDI
101526	<input checked="" type="checkbox"/>	18/07/2014	US\$	20,720.00	250,000.00	CABRAL	C. KAUFMAN	470 910	HEXA TRADE LI...	TRIDENT CHAMBE...	BANQUE AUDI
101555	<input checked="" type="checkbox"/>	24/07/2014	US\$	510,864.86	0.00	CABRAL	MER12	116 310 669 1	NEW BOXER IM...	29/26 26TH EKAMAI	BANGKOK BAN...

Mostrar ORDENES: DIA Anterior 50 Busqueda A Buscar: cabral Buscar Desde: 01/01/2007 E

Borrar Orden Borrar Visual Agregar Orden Nueva

Figura 06

Já na página 704 do mesmo documento, emitido pela 7ª Vara Federal Criminal do Rio de Janeiro, pode ser observar a tela reproduzida na Figura 07.

BankDrop v2.0.50727.8825 en RP-021876

Favorecido
 Nombre: **NEW BOXER IMPORT EXPORT CO LTD**
 Direccion: **29/26 26TH EKAMAI SOI, SUKHUMWIT 6**
 NoCuenta: **116 310 669 1**
 Web: <http://www.newboxer.com/2007/pressroom-p>

Banco Beneficiario
 Nombre: **BANGKOK BANK PUBLIC COMPANY LIMITED**
 Direccion: **333 SILOM ROAD, BANGRUK**
 Estado: **BANGKOK**
 País: **THAILAND**
 Swift: **BKKBTHBKXXX**

Banco Intermediario
 Nombre: **BANGKOK BANK PUBLIC COMPANY LTD**
 Estado: **NEW YORK**
 País: **USA**
 Swift: **CHASUS33XXX**

Datos
 Cliente: **CABRAL** BK **MER12** Fecha **24/07/2014**
 Valor **US\$ 510,864.86**
 Referencia **S14-780 / S14-801**
 Motivo: **Importacion Textil**

Formato Texto
 Banco: **BANGKOK BANK PUBLIC COMPANY LIMITED**
 BANGKOK/THAILAND
 Swift: **BKKBTHBKXXX**
 End : **333 SILOM ROAD, BANGRUK**

Seguimiento
 29/07/2014 - CARMEN
 (10:20:56 AM) Cabral: blz (10:21:03 AM) Cabral: New Boxer chegu (10:22:09 AM) emmacatt2014@gmail.com/0935C22C: Blz...os 510 e quebrados, ne ? (10:22:24 AM) emmacatt2014@gmail.com/0935C22C: 510 865 (10:23:20 AM) Cabral: isto mesmo (10:26:06 AM)

Ingreso **PATY 24/07/2014** Modificado **ANDREA 28/07/2014**

ID	Confirm	Fecha	Mon	Valor	Total Orden	Cliente	BK	Fav.Cuenta	Fav.Nombre	Favorecido Direccion	Banco
96470	<input checked="" type="checkbox"/>	26/07/2011	US\$	350,000.00	450,000.00	CABRAL	TUTA	OSA 110 081 640 478...	D AND C FORT...	RM 907 JYW 189, W...	SHENZHEN DEV...
99644	<input checked="" type="checkbox"/>	23/04/2013	US\$	366,333.00	0.00	CABRAL	SALIBA	546 494	PRINCETON NO...	WOODBOURNE HA...	EFB BANK AG
92653	<input checked="" type="checkbox"/>	30/11/2009	US\$	400,000.00	0.00	CABRAL	GIL0	424 400	FENDE HOLDIN...	SWISS TOWER, 16...	BANQUE AUDI
102134	<input checked="" type="checkbox"/>	26/11/2014	US\$	400,000.00	0.00	CABRAL	PEDRA	283 78	LEGACY UNIVE...	10 BLVRD ROYAL L...	BANK HAPOLI...
103089	<input checked="" type="checkbox"/>	05/11/2015	US\$	401,243.00	0.00	CABRAL	MOLLEJAPEN	788 397 073 883	SWEN R2 LIMIT...	SUITE 2212 22F TO...	HANG SENG BA...
99158	<input checked="" type="checkbox"/>	19/12/2012	US\$	454,648.74	0.00	CABRAL	LUXO	626 649 060 333	RASAN ASSOCI...	2 COURS DE RIVE 1...	BARCLAYS BANK
97471	<input checked="" type="checkbox"/>	03/02/2012	US\$	480,000.00	0.00	CABRAL	CURIO	OSA 110 081 640 478...	D AND C FORT...	RM 907 JYW 189, W...	SHENZHEN DEV...
97514	<input checked="" type="checkbox"/>	15/02/2012	US\$	480,000.00	0.00	CABRAL	CURIO	OSA 110 081 640 478...	D AND C FORT...	RM 907 JYW 189, W...	SHENZHEN DEV...
100684	<input checked="" type="checkbox"/>	17/12/2013	US\$	500,000.00	0.00	CABRAL	PEDRA	565 999	MIVEX TRADIN...	SWISS TOWER, 16...	BANQUE AUDI
101555	<input checked="" type="checkbox"/>	24/07/2014	US\$	510,864.86	0.00	CABRAL	MER12	116 310 669 1	NEW BOXER IM...	29/26 26TH EKAMAI	BANGKOK BAN...

Figura 07

É interessante observar que ambas as telas têm, evidenciada/selecionada (em cor azul), uma suposta transação de número 101555, que teria ocorrido em 24/07/2014 no valor de US\$ 510.864,86 (detalhe 1 nas Figuras 06 e 07).

Ocorre que de acordo com a tela da Fig. 06 (detalhe 2) a transação evidenciada teria sido digitada e modificada por uma tal de “Carmen” em 18/07/2014 enquanto na tela da Fig. 07 (detalhe 2) a transação evidenciada (em cor azul) teria sido digitada por “Paty” em 24/07/2014 e modificada por “Andrea” em 28/07/2014.

Inclusive a primeira tela apresenta um campo adicional “confirmado” (detalhe 3 da Fig. 06) que não existe na segunda tela.

Ademais na segunda tela (Fig. 07) também estão ausentes uma série de botões e outras informações, na parte inferior, que aparecem na primeira tela (detalhes 5 na Fig. 06).

Isso sem contar, que as versões dos dois softwares são diferentes (como já descrito na resposta ao Quesito 7), sendo a primeira a v. 2.0.50727.8794 que funcionava no computador “Desktop” com o usuário “Khadjdf” enquanto a segunda seria a v. 2.0.50727.8825 que funcionava no computador “RP” com usuário “021876” (detalhe 4 nas Fig. 06 e 07).

Isso significa que, caso o suposto sistema Bankdrop exista realmente, além de existirem diversas versões do mesmo, existem também diversas versões dos dados e das informações subjacentes que, pelo exposto acima não têm, evidentemente, qualquer tipo de controle de integridade e, por consequência, não podem ser considerados como dignos de credibilidade e, menos ainda, como fonte de qualquer tipo de comprovação.

Se trata, ao que tudo indica, de informações inseridas de forma espúria e sem qualquer tipo de controle, em datas aleatórias e, por óbvia consequência, sem efetiva conexão com a realidade dos fatos.

Como se pode confiar em informações desta natureza, com tão patentes inconsistências, e, pior, considerar as mesmas como provas válidas?

Com relação ao Documento B a situação é ainda pior pois, como já detalhado na resposta ao Quesito 9, a falsificação de um documento em formato texto, como é o caso do Documento B, é de extrema simplicidade e não requer qualquer habilidade especial. Vale ainda ressaltar a inconsistência entre data de produção do Documento B e data indicada como momento da extração dos dados do suposto software, detalhada na resposta ao Quesito 15 (Fig. 17).

Conforme descrito na resposta ao Quesito 9, para mero fim de exemplo foi produzido um arquivo PDF com as mesmas idênticas características do Documento B (inclusive os metadados) no qual foi simplesmente substituído o codinome “CABRAL” pelo codinome “XXXXXX”.

Não há qualquer elemento, nos autos, que permita dizer que o Documento B não tenha sido produzido desta mesma forma, usando informações e dados inventados ou falsos, em tudo ou em parte, possivelmente na mesma data de criação do arquivo PDF (29/01/2018).

De fato, pode-se dizer que o mencionado documento “*exemplo_falso.pdf*” criado por nós a título de exemplo, à luz dos elementos presentes nos autos até o momento, tem as mesmas características e é tão “autêntico” quanto o documento em formato PDF (Documento B) do suposto software “ST” apresentado pelos colaboradores e utilizado pelo MPF em sua denúncia.

Tudo quanto acima serve para demonstrar como, na ausência de uma origem certa e de uma cadeia de custódia sólida e/ou de uma adequada e segura forma de autenticação, é extremamente difícil e arriscado aceitar documentos eletrônicos como autênticos e verídicos.

Por esta razão o moderno CPC, em seus Artigos 439 e 441, determina especificamente que a aceitação de documentos eletrônicos depende “**da verificação de sua autenticidade, na forma da lei**”, desde que tenham sido “**produzidos e conservados com a observância da legislação específica**”.

• Resposta ao Quesito 11.

A qualidade das imagens presentes nos Documento A é relativamente baixa, possivelmente devido a compressão gráfica realizada para a codificação do arquivo em formato PDF.

Tais imagens foram aparentemente comprimidas no padrão JPG (normalmente utilizado nos arquivos PDF), provavelmente com taxa de compressão ao redor de 75%, presumivelmente na fase de criação do arquivo PDF.

Os tipos de análise que podem ser realizados, em relação ao Documento A, nestas condições são essencialmente uma análise ELA sobre as imagens que formam o documento e uma análise geral de detalhes gráficos.

Análise ELA

O estudo das imagens com a técnica ELA (Error Level Analysis) permite detectar áreas onde houve variação do nível de compactação da imagem (que resulta em diferente resolução), por esta razão esta análise funciona em imagens que usam compressão com perdas de qualidade (*lossy*), como o clássico formato JPG.

Conforme explicado detalhadamente na resposta ao Quesito 15, o Documento A é formado integralmente por imagens que foram provavelmente criadas no formato PNG (compressão sem perdas) e sucessivamente convertidas ao formato JPG na hora da criação do arquivo PDF.

Adicionalmente, o software de simulação de impressora utilizado para criar o arquivo PDF (PDFCreator 2.5.2.5233) dividiu cada imagem horizontalmente (como se pode verificar simplesmente tentando selecionar uma qualquer imagem do Documento A, e observando que somente será selecionada a parte superior ou inferior, sendo a imagem dividida em duas - Fig. 08).

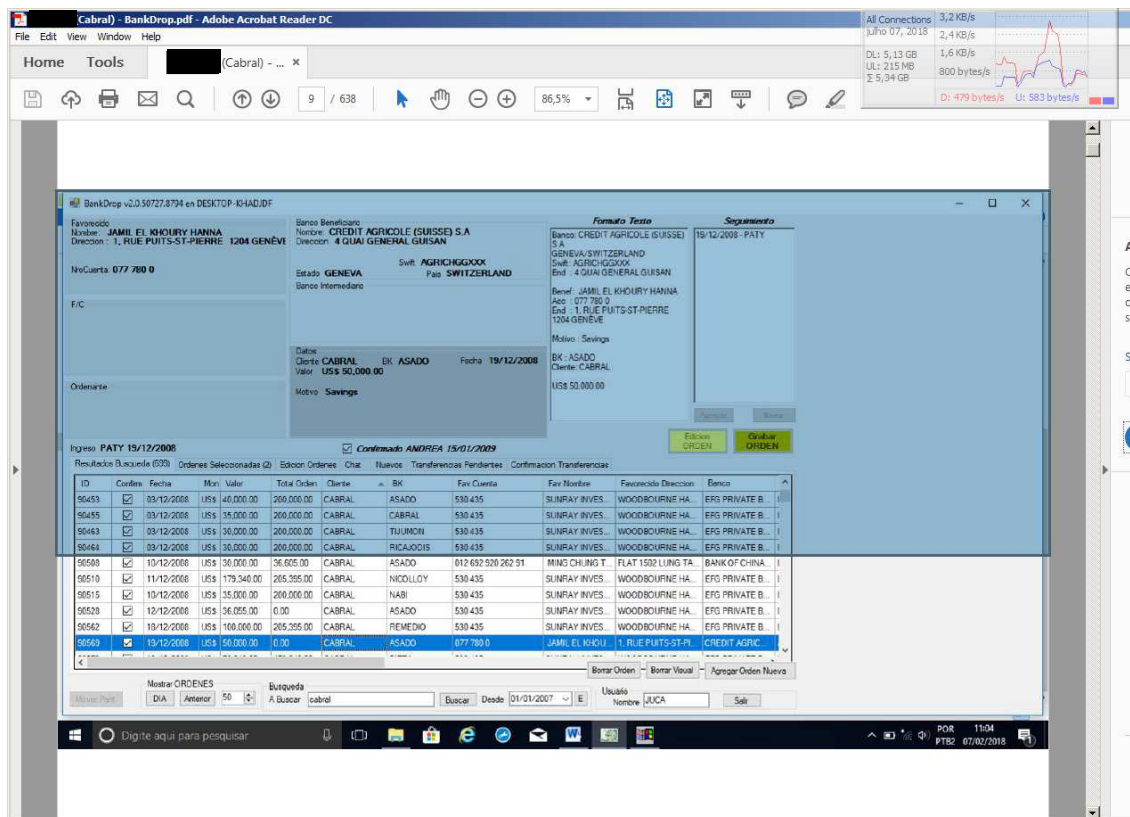


Figura 08

Foi selecionada, para análise ELA, uma das imagens do Documento A, no caso a imagem presente na página 09.

Como acontece nas demais páginas do Documento A, e já explicado acima, a imagem que aparece nesta página é dividida horizontalmente em duas partes (Fig. 09 e Fig. 11).

Foram então analisadas ambas as partes através de estudo ELA realizado por meio do software forense Ghiró.

Os resultados, que ficaram em cores muito escuras (como previsível e explicado mais a frente) foram tratados para aumentar a luminosidade em 40%, de forma que os detalhes fossem mais visíveis, e estão reproduzidos, na versão mais luminosa, respectivamente nas Figuras 10 (ELA relativo a Fig. 09) e 12 (ELA relativo a Fig. 11).

Lorenzo Parodi

Perito em fraudes e falsificações



Figura 09

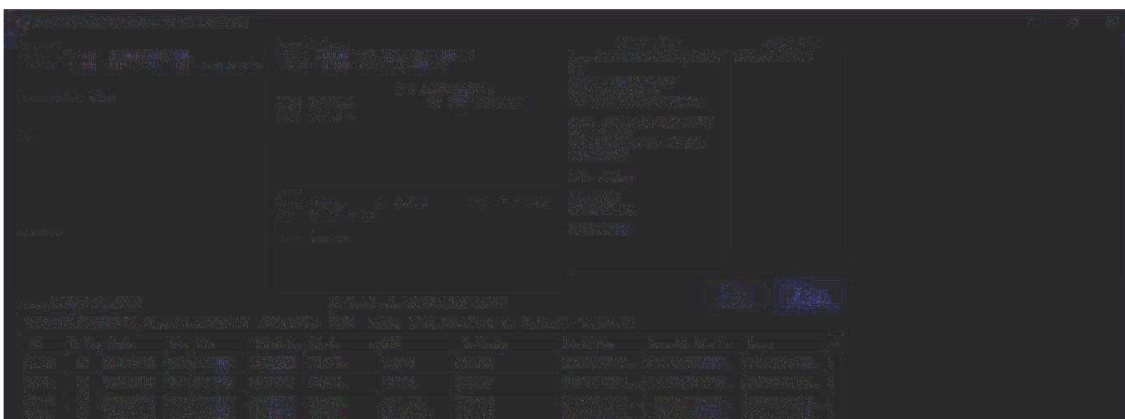


Figura 10

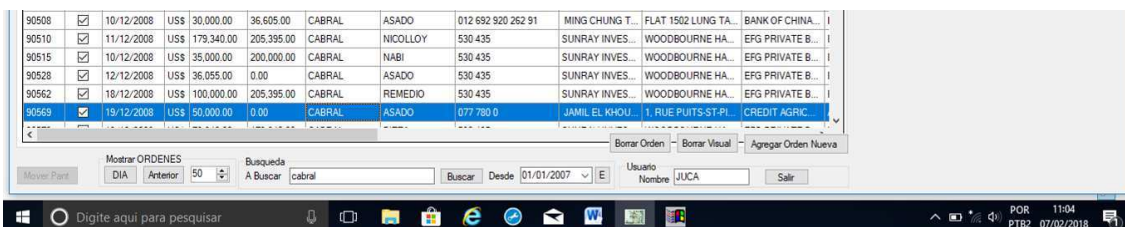


Figura 11



Figura 12

De fato o estudo ELA não conseguiu revelar indícios suficientes para afirmar que tenha havido adulterações.

Isso pode, inclusive, ser devido ao fato que as imagens que originaram o arquivo PDF eram inicialmente em formato PNG, que é um formato de compressão sem perdas de qualidade (lossless), como verificado na resposta ao Quesito 15 (detalhes 3 da Fig. 14).

Nesse tipo de arquivo PNG, após ser convertido ao formato JPG (como ocorre normalmente quando se cria um arquivo PDF a partir de imagens), são virtualmente eliminadas todas as características de uma eventual edição, que podem ser destacadas pela técnica ELA. Somente edições posteriores, eventualmente realizadas no arquivo quando já em formato JPG, poderiam ser relevadas.

De fato, as únicas conclusões com algum grau de confiabilidade em relação aos arquivos de imagem no documento A é que, provavelmente, tenham passado por mais de um ciclo de compressão, ou seja por mais de uma sequência de abertura/elaboração e salvamento. Isso se deduz em função da predominância de amplas áreas muito escuras (pretas) na análise ELA.

Análise de Detalhes Gráficos

Com uma observação atenta dos diversos detalhes das imagens que formam o Documento A, se podem perceber, em alguns pontos, variações notáveis, dentro da mesma imagem, sobretudo no padrão de coloração e fundo.

Uma das possíveis razões de tais variações é a ocorrência de edição gráfica (que pode ser tanto operações de copia-cola, quanto remoções ou alterações diretas), que pode ter ocorrido nos campos que possuem tais variações.



Figura 13

Na já mencionada imagem presente na página 09 do Documento A (por exemplo), comparando o formato do fundo do campo demarcado com o detalhe 1 (Fig. 13) em relação ao fundo dos campos demarcados com os detalhes 2 (Fig. 13), na mesma linha e imagem, pode-se perceber uma consistente diferença de padrão e de cores, que é difícil de explicar considerando que se trata da mesma imagem, da mesma linha e, em tese, das mesmas cores.

Com relação ao Documento B não há imagens a serem analisadas pois, conforme já amplamente explicado, este arquivo/documento é formado exclusivamente por texto formatado e não por imagens. O texto, como já demonstrado, pode ser facilmente alterado mas não há como comprovar que isso tenha ocorrido baseado somente no arquivo fornecido.

Por tudo quanto acima, com base nos arquivos e informações disponíveis nos autos do processo em foco, e mesmo existindo indícios de possíveis edições ou alterações dos arquivos de imagens, não é possível afirmar que os mencionados documentos (Documento A e Documento B) tenham sido certamente objeto de edição ou alterações.

Da mesma forma **não há, nos autos, qualquer elemento minimamente suficiente para que se possa afirmar que tais documentos sejam autênticos** (pelo contrário, há diversos elementos que suscitam suspeitas e dúvidas).

- **Resposta ao Quesito 12.**

As modalidades das possíveis alterações nos Documentos A e B foram detalhadamente descritas na resposta ao Quesito 11.

É oportuno ressaltar, mais uma vez, que o material disponível nos autos é insuficiente e inapto para comprovar a existência de alterações ou edições, sendo tão somente suficiente para comprovar que tais alterações ou edições seriam perfeitamente possíveis (como já demonstrado).

Da mesma forma o material presente nos autos é certamente insuficiente e inapto para comprovar a autenticidade dos documentos em foco.

- **Resposta ao Quesito 13.**

Conforme detalhadamente exposto na resposta ao Quesito 10, os Documentos A e B, no estado em que se encontram, poderiam facilmente ter sido falsificados (como inclusive comprovado com a elaboração de uma versão editada do Documento B, em tudo comparável àquela presente nos autos).

Na impossibilidade de analisar detalhadamente o eventual software de origem (em todas suas versões, com relativos dados e nos computadores/sistemas de origem, conforme detalhado na resposta ao Quesito 7) e na ausência de uma sólida comprovação da cadeia de custódia destes sistemas (ver resposta ao Quesito 14), é **certamente impossível considerar tais documentos como aptos a comprovar qualquer coisa.**

De fato, por sua extrema (e comprovada) facilidade de falsificação, ausência de origem comprovada, ausência de meios de autenticação e ausência total de cadeia de custódia, estes documentos, em sua forma atual, podem ser considerados como absolutamente ineficazes para fornecer ou comprovar qualquer tipo de informação minimamente consistente e crível.

- **Resposta ao Quesito 14.**

Destarte é oportuno definir o que se entende, normalmente e de acordo com as melhores práticas, por “cadeia de custódia”.

Cadeia de Custódia é o processo de documentar a história cronológica do vestígio, do indício ou da prova, esse processo visa a garantir o rastreamento das provas utilizadas em processos judiciais, registrar sua origem e quem teve acesso ou realizou o manuseio desta prova.

No que diz respeito à preservação das informações coletadas, a cadeia de custódia possibilita documentar a cronologia das provas, qual sua origem, quem foram os responsáveis por seu manuseio e garantir a inviolabilidade do material, tudo isso para evitar a **perda da confiança do elemento probatório**.

Como ensina Geraldo Prado (“Prova penal e sistema de controles epistêmicos”, 2014, pag. 55), no atual processo penal *“Não há mais espaço para a admissão acrítica das acusações penais, pois a ordem jurídica, observada pelos mais diversos ângulos, convoca a jurisdição ao exame não apenas da justa causa para a ação penal, como também da **legalidade da atividade anterior, preparatória, indagando sobre a estrita legalidade da obtenção e preservação dos meios de prova - isto é, da escrupulosa legalidade do acesso às fontes de prova e da manutenção destas fontes em condição de serem consultadas, oportunamente, pelas partes.**”*. [grifos nossos]

Entretanto, apenas conhecer a fonte inicial da prova e a legalidade da sua obtenção (no caso, já questionada na resposta ao Quesito 16) não é suficiente, é necessário que se conheça a integralidade da cadeia de custódia.

No caso em foco não há qualquer elemento que indique a consistência da cadeia de custódia dos documentos descritos no escopo do presente laudo.

Os documentos em questão têm origem desconhecida, pois não é possível sequer comprovar a existência dos softwares mencionados pelos colaboradores como sendo sua origem, não havendo acesso ao computador onde estes supostos softwares funcionariam nem sendo disponíveis cópias confiáveis dos mesmos e de seus dados.

Conforme descrito mais detalhadamente na resposta ao Quesito 15, o “Documento A” foi criado a partir de imagens salvas em um computador, alegadamente capturadas a partir do mencionado software, mas que poderiam muito bem ter sido criadas diversamente ou editadas de várias formas antes de serem “impressas” no arquivo PDF.

Não há tanto no documento em formato PDF (Documento A) quanto nas imagens que o compõem, qualquer elemento que permita indicar qual a real origem de todas as informações aí presentes, como elas foram formadas, quando, quem e onde as coletou, quem as manuseou e conservou e como, qual processo foi realmente utilizado para formar o conjunto de informações e quais garantias existam quanto a sua integridade e veracidade.

A situação relativamente ao “Documento B” é, se possível, ainda mais duvidosa. Se trata de um documento criado, desde sua origem, em formato “texto”. Isso quer dizer que pode ter como fonte um qualquer arquivo de texto (formato TXT) criado, editado e impresso em PDF em qualquer tempo, por qualquer pessoa que tenha acesso a um banalíssimo editor de texto, como o famoso “notepad” disponível gratuitamente no sistema Windows.

Não há a mínima indicação de qual seja sua efetiva origem e autoria, fora as escassas, não confiáveis, e pouco relevantes informações contidas nos metadados do arquivo PDF, mencionados na resposta ao Quesito 3.

Não é sequer possível dizer se os arquivos foram de alguma forma acessados ou modificados indevidamente uma vez que entregues ao Ministério Público Federal, pois não foi fornecido nenhum tipo de documento e comprovação das condições em que estes foram entregues ao MPF (por exemplo, um comprovante do HashCode SHA-256 do HD inteiro no momento da entrega, autenticado quanto a sua data por um cartório de notas ou por uma assinatura eletrônica com carimbo de data realizado por agente autorizado da ICP-Brasil) e de como e por quem tais informações foram tratadas posteriormente, até serem apresentadas ao Juízo.

Na realidade, salvo melhor juízo, a **situação atual** dos arquivos eletrônicos em foco é de **ausência total de uma mínima comprovação de sua real origem e da existência de uma cadeia de custódia dos vestígios** (os documentos eletrônicos) e demais informações, em todo o período anterior à data de apresentação em juízo de tais documentos e relativa juntada nos autos, o que eiva de graves dúvidas a legalidade da atividade anterior à ação penal.

• Resposta ao Quesito 15.

O processo de análise pericial de documentos utiliza técnicas variadas. Um dos métodos frequentemente usados é a comparação detalhada do documento questionado com outros similares, em tudo ou em parte, e certamente autênticos, o que, no caso em foco, não é possível, por não existir nenhum documento comparável e certamente autêntico, nem outros elementos verificáveis, quais escritas manuais, assinaturas, autenticações, carimbos etc.

Por estas razões, toda a análise deve se restringir a características lógicas, gráficas e de composição e formato dos arquivos.

De antemão é oportuno explicar que os arquivos em formato PDF (Portable Document Format, padrão criado pela empresa Adobe em 1993) são compostos por objetos distintos (imagens, textos, notas etc.) que são “fundidos” em um único documento legível por qualquer dispositivo (por isso portátil).

De fato, porém, em seu interior, tais arquivos mantêm os objetos separados e identificados individualmente (mesmo que, em alguns casos, criptografados ou de outra maneira codificados).

Além disso os arquivos PDF contêm os chamados “metadados” (*metadata*, em língua inglesa), ou seja, um conjunto de informações adicionais, gravadas no arquivo, que dizem respeito, por exemplo, à sua data e hora de origem, autor, software de criação, eventuais modificações etc.

É importante mencionar que os metadados podem ser objeto de edição e alteração, através de apropriadas ferramentas softwares.

Por esta razão é perfeitamente possível, por exemplo, criar um arquivo em uma data e gravar nos metadados que o arquivo foi criado em outra data.

Pela análise realizada os documentos em questão foram criados:

- a) O Documento A, a partir de imagens arquivadas localmente em um computador, sem qualquer conteúdo de texto (detalhes 1 na Fig. 15, lado esquerdo).
- b) O Documento B, a partir de simples texto, sem imagens (detalhes 1 na Fig. 15, lado direito).

Ambos os documentos foram criados por impressoras PDF, ou seja softwares que simulam uma impressão transferindo o conteúdo que deveria ser impresso para um arquivo digital criado de acordo com o formato PDF.

Se deduz que o Documento A foi criado a partir de imagens arquivadas localmente, observando a imagem presente na página 379 do mencionado documento (Fig. 14).

Nela aparece de forma evidente, em transparência, uma pasta denominada “Anexo 46 – [REDACTED] (Cabral)” (detalhes 1 na Fig. 14) a qual, de acordo com a tela capturada, contém 321 arquivos (detalhe 2 na Fig. 14).

Todos os arquivos que aparecem, em transparência, são arquivos gráficos em formato PNG (um dos vários formatos gráficos existentes), denominados como “*Captura de tela (XXXX).png*” (detalhe 3 na Fig. 14), onde XXXX é um número que aparenta ser sequencial e na ordem dos diversos milhares.

Interessante observar que a orientação das imagens presentes no Documento A, registrada na criação do arquivo PDF, é vertical (“*portrait*” - detalhe 2 na Fig. 15, lado esquerdo), ou seja não aquela natural das telas supostamente capturadas.

Isso comprova que, de fato, o arquivo foi gerado a partir de imagens previamente arquivadas (e possivelmente elaboradas ou alteradas, antes de serem “impressas” no arquivo PDF) e não diretamente do suposto software “Bankdrop” que teria gerado tais imagens.

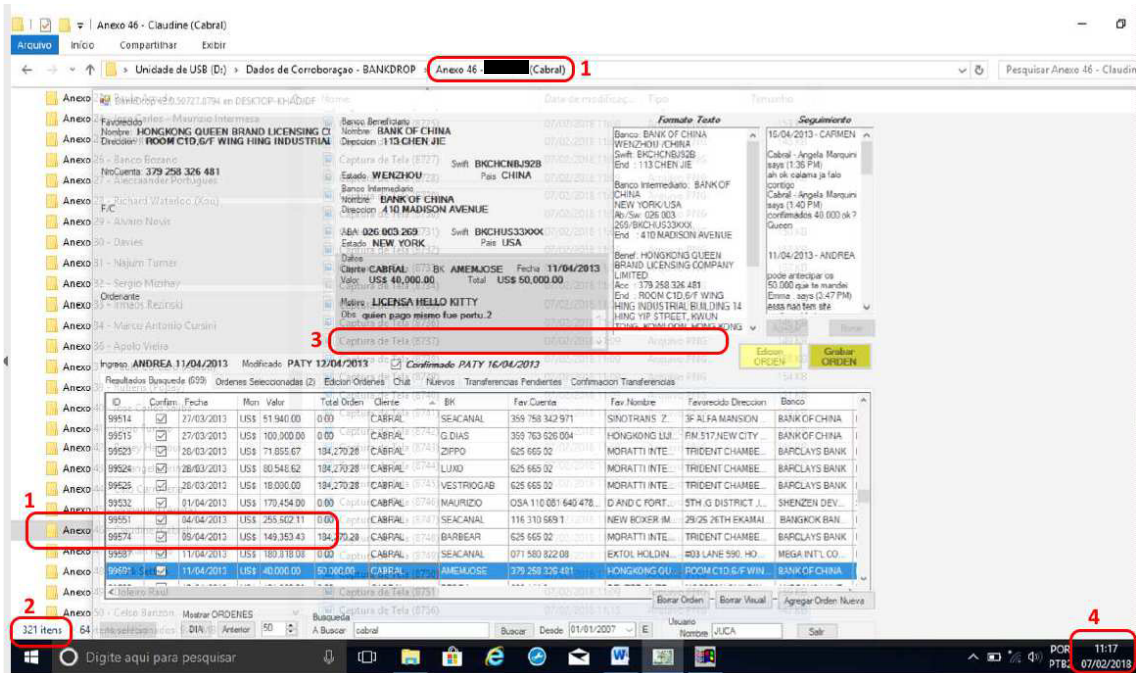


Figura 14



Figura 15

Quanto ao Documento B, ele não contém nenhuma imagem e os metadados do arquivo PDF indicam que é composto por mero texto (detalhe 1 na Fig. 15, lado direito), sem qualquer outra indicação quanto a sua origem. A orientação das telas, porém, é a horizontal, diversamente do Documento A.

Pode-se dizer, ainda, que os dois arquivos ou documentos eletrônicos foram muito provavelmente criados a partir de computadores diferentes e por pessoas diferentes, por lógica consequência das seguintes diferenças, extraídas dos metadados dos respectivos arquivos PDF:

- 1) O Documento A consta como criado utilizando o software de impressão "PDFCreator 2.5.2.5233" (detalhe 1, Fig. 16, lado esquerdo), tem como autor um usuário "Atendimento" (detalhe 2, Fig. 16, lado esquerdo) e foi criado em 22/02/2018 (detalhe 3, Fig. 16, lado esquerdo).

- 2) O Documento B foi criado a partir do software de impressão “Microsoft: Print To PDF” (detalhe1, Fig. 16, lado direito), tem como autor um usuário “Advogado” (detalhe 2, Fig. 16, lado direito) e foi criado em 29/01/2018 (detalhe 3, Fig. 16, lado direito).

Document A		Document B	
Document Statistics			
Number of Attachments	0	Number of Attachments	0
Number of Bookmarks	0	Number of Bookmarks	0
Number of Destinations	0	Number of Destinations	0
Number of Form Fields	0	Number of Form Fields	0
Number of Pages	638	Number of Pages	41
File Details			
Metadata			
Author	Atendimento	Author	Advogado
Created On	D:20180221175259-03'00'	Created On	D:20180129133255-02'00'
Keywords		Keywords	
Last Modified	D:20180221175259-03'00'	Last Modified	D:20180129133255-02'00'
PDF Creator	PDFCreator 2.5.2.5233	PDF Creator	
PDF Producer	PDFCreator 2.5.2.5233	PDF Producer	Microsoft: Print To PDF
Subject		Subject	
Title	Foto de página inteira	Title	ST
PDF Details			
Page Rotation	0 degrees	Page Rotation	0 degrees
Page Size	8,263889 by 11,69444 inches, 20	Page Size	11,69333 by 8,268333 inches, 29
PDF Version	1.4	PDF Version	1.7

Figura 16

Existem, nos Documentos A e B, diversas incongruências e inconsistências lógicas que geram suspeitas e dúvidas e, certamente, merecem um aprofundamento (impossível com os escassos elementos presentes nos autos). Os pontos principais a serem observados, são indicados a seguir:

- a) O Documento B, em todas suas páginas (em alto a esquerda) reporta como data de “emissão” a data “Quarta-feira, 16 de novembro de 2016” (detalhe 1 na Fig. 17).

DATA	TIPO	ORIGEM	DESTINO	VALOR DOLAR	VALOR REAL USUARIO	TxBASE	OBS
001-RJ							
Quarta-feira, 16 de novembro de 2016 1							
MOVIMENTOS FILTRADOS (ENTRADAS)							
Pag.: 0001/0041							
FILTROS:							
1 - Compra 2 - Venda 3 - Tr R\$ 4 - Tr US 5 - Obs R\$ 10 - ObsUS\$							
Conta origem: CABRAL Conta destino: (TODOS) Data: 01/01/2011 até 16/11/2016							
RP/OBS: Lançado por: 0 - (TODOS) OBS por: 0 - (TODOS)							
CLASSIFICADO POR: DATA, TIPO, ORIGEM E DESTINO							
12/01/2011	04-Tr	US\$ CABRAL	TIJUMON	60,000.00	0.00	32	CARMENCITA SINCLAIR - NANDAMOS 40MIL A MAIS
OBS2: 42PAT CONF 27/01							
19/01/2011	02-Venda	CABRAL		50,000.00	86,500.00	39	FOGO 1.73 DH / OP Q FALTAVA LANCAR
04/02/2011	02-Venda	CABRAL		100,000.00	173,000.00	23	BETH 1.73 ACERTO BATIDO COM MEDIADOR // FECHA
MENTO DA DATA 03/01							
09/02/2011	03-Tr	R\$ CABRAL	CABRALDEV	0.00	1,743.04	23	BETH

Figura 17

Ocorre que o Documento B, de acordo com os metadados do arquivo PDF, foi criado em 29 de janeiro de 2018 (detalhe 3 na Fig. 16, lado direito), ou seja, mais de dois anos depois da data indicada nas páginas do Documento B.

Isso indica que, caso realmente originados pelo suposto software indicado pelos colaboradores, os textos que compõem o Documento B foram extraídos do software em 2016 e armazenados provavelmente em algum arquivo eletrônico em formato texto (TXT).

Somente dois anos mais tarde, em 2018, oportunamente, tal arquivo texto foi transformado em um arquivo PDF, sem qualquer garantia que nestes dois anos alguém tenha editado os dados nele contidos (coisa extremamente fácil de se fazer em um arquivo de texto, normalmente identificado com o sufixo TXT), ou seja, sem qualquer comprovação da existência de uma cadeia de custódia de tais informações.

- b) Na já mencionada página 379 do Documento A, conforme descrito anteriormente, aparecem listados 321 arquivos de imagem (imagens estas supostamente capturadas de algum software ou criadas através de algum programa de gráfica), verossimilmente e aparentemente utilizados para compor o arquivo PDF do Documento A. Ocorre que o Documento A é composto por 638 páginas. Se 321 destas páginas vieram das imagens salvas na pasta que aparece na mencionada página 379 do Documento A (detalhe 1, Fig. 14), resta descobrir de onde vieram as demais 317 páginas, quem as produziu, como e quando?
- c) De acordo com a data do computador que aparece em todas as telas do Documento A (detalhe 4 na Fig. 14), o trabalho de impressão teria ocorrido no dia 07/02/2018. De acordo com os metadados do Arquivo PDF correspondente ao Documento A, porém, o mesmo foi criado no dia 21/02/2018 (detalhe 3 na Fig. 16, lado esquerdo), restando a dúvida quanto ao que aconteceu com este arquivo ou com as imagens que o compõem, entre os dias 07/02/2018 e o dia 21/02/2018.

Como foram conservadas as imagens e talvez o arquivo PDF, o que garante que não passaram por edições (eliminando, adicionando ou modificando informações) etc.?

- d) Interessante, ainda, observar que a estrutura das telas que compõem o Documento A é redigida em língua espanhola (detalhes 1 na Fig. 18, como exemplo). Já todas as demais supostas informações e anotações contidas em tais telas são em língua portuguesa (detalhe 2 na Fig. 18).

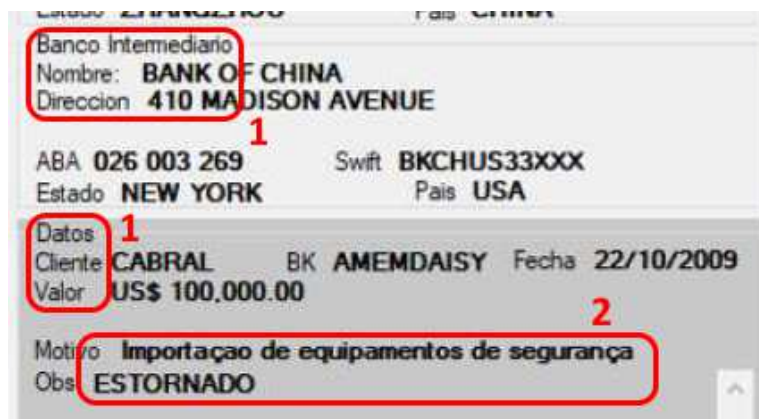


Figura 18

Sem querer, neste momento, entrar no mérito da necessidade de tradução oficial do Documento A, de acordo com o Art. 236 CPP, isso cria a curiosa situação pela qual alguém teria criado um software em espanhol para depois usá-lo no Brasil.

Ou, em outra possível leitura, talvez alguém tenha introduzido dados de seu interesse, em língua portuguesa, em um software estrangeiro que tinha outra finalidade e destino? Somente uma análise pericial detalhada do sistema informático original, com relativos supostos softwares e dados, poderia dirimir esta dúvida.

Ademais os dois supostos softwares, que em tese deveriam ser operados em conjunto, são um em língua espanhola (como já indicado) e o outro (aquele denominado “ST”, que teria gerado o Documento B) integralmente em língua portuguesa, criando uma verdadeira contradição quanto a sua efetiva origem e interoperabilidade.

Por tudo quanto acima, com base nos arquivos e informações disponíveis nos autos do processo em foco, **certamente não é possível afirmar que os mencionados documentos (Documento A e Documento B) sejam autênticos e não foram objeto de eventuais adulterações ou edições.**

Pelo contrário, existem diversos indícios que permitem considerar a concreta possibilidade que os Documentos A e B tenham sido objeto de adulterações, ao menos no que diz respeito ao teor das informações em seu conteúdo.

- **Resposta ao Quesito 16.**

Destarte, é inevitável salientar, nesta análise, que o processo em foco é um processo penal, sujeito portanto, obviamente, as regras deste ramo do direito, inclusive e especialmente no que diz respeito às normas processuais.

A questão das provas, e de sua validade, no direito penal é regida principalmente pelos Artigos 155 a 159 do Código de Processo Penal. Importante frisar, em relação a este ponto, que o CPP foi instituído em 1941 e que, apesar de algumas atualizações ocorridas em 2008, ainda está estruturalmente ligado a uma realidade ultrapassada em várias questões, em particular em relação a tudo que diz respeito à crescente digitalização das relações no mundo de hoje.

O processo penal, por consequência de seu alcance que pode atingir direitos fundamentais do Réu (até mesmo sua liberdade), está sujeito a regras muito mais estreitas e garantias mais rigorosas em relação a outros ramos do direito.

A própria Constituição Federal (em especial em seu artigo 5º), coloca o ser humano como o centro de todas as preocupações e por isso dispõe princípios pétreos entre os quais o do “Devido Processo Legal”, ou seja, do processo que **deve** ser realizado preservando todos os direitos do Réu, permitindo sua “ampla defesa” e aplicando estritamente todas e somente as normas aplicáveis.

No caso em foco, evidentemente, os documentos objeto desta análise constituem vestígios de um suposto crime e, como tais, fazem parte do corpo do delito e estão sujeitos, para sua validação como provas e sua consequente valoração por parte do Juízo, às regras definidas pelo Art. 158 CPP, o qual determina que *“Quando a infração deixar vestígios, **será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.**”*. [grifo nosso]

Ou seja, **antes de poder ser considerado como prova válida**, qualquer vestígio deve ser submetido a perícia oficial, podendo as partes formular quesitos (conforme Art. 159, § 3 CPP), para estabelecer e comprovar, entre outros, sua relação inquestionável com o fato e com as pessoas envolvidas, sua efetiva origem, sua autenticidade e integridade além da existência de uma cadeia de custódia consistente desde sua origem.

Pela análise dos autos **nada disso foi feito** em relação aos documentos em foco. Já somente por esta razão, entendo que os mencionados documentos, até o presente momento, não podem ser considerados como provas válidas nem podem ser utilizados para embasar qualquer tipo de decisão judicial.

Importante observar que, de acordo com o Art. 564, inc. III, b) CPP, a omissão, por parte do Estado, na realização do exame pericial oficial dos vestígios que formam o corpo do delito, **é causa para nulidade absoluta do processo**.

Adicionalmente, por se tratar de documentos em formato eletrônico e considerando que o atual vetusto CPP não trata especificamente deste tipo de vestígio, entendo que pode ser aplicado, *in bonam partem*, por sua maior especificidade e modernidade neste âmbito, o CPC/15 que, em seus Artigos 439 e 441, determina o seguinte:

*“Art. 439. A utilização de documentos eletrônicos no processo convencional dependerá de sua conversão à forma impressa e **da verificação de sua autenticidade, na forma da lei.**”* [grifo nosso]

“Art. 441. Serão admitidos documentos eletrônicos produzidos e conservados com a observância da legislação específica.”

Vicente Greco Filho, em sua obra sobre “Direito Processual Civil”, define o documento como todo objeto do qual se extraem fatos em virtude da existência de símbolos ou sinais gráficos, mecânicos, eletromagnéticos etc.

Ainda, de acordo com o Art. 232 CPP *“Consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares.”*

Por conseguinte, o termo “documento eletrônico” compreende escritos ou registro de fatos que têm como meio físico um suporte eletrônico ou digital, quais sejam, os dispositivos e sistemas que armazenam informações: CDs, DVDs, HDs, pen-drives, e-mail e arquivos digitais em geral.

No caso em foco, novamente, os documentos eletrônicos, “Documento A” e “Documento B”, acima descritos, não passaram por qualquer processo de verificação de sua autenticidade e também não foram produzidos e conservados com observância da legislação.

No caso, sequer se pode saber com certeza onde, quando, por quem e a partir de qual software foram produzidos, nem como e por quem foram “conservados” após sua produção.

Por estas razões, os Documentos A e B, no estado atual, **certamente não podem ser admitidos como provas válidas.**

O Art. 5, inc. LVI da CF e o Art. 157 CPP, definem a inadmissibilidade, no processo penal, das provas obtidas por meios ilícitos.

Ora, se não se conhece ao certo a real origem dos documentos em foco, nem se tem acesso ao suposto software que teria originado tais documentos (se é que tal software realmente existe), como se pode ter certeza que os tais documentos não foram obtidos por meios ilícitos (por exemplo, invadindo um computador, ex Art. 154-A CP, o que parece ser uma hipótese perfeitamente possível e plausível)?

É imperativo, ainda, observar que **existem diversos elementos suspeitos e fatores que permitem admitir a possibilidade de adulteração** nos documentos sob análise, descritos mais detalhadamente nas respostas aos Quesitos 10, 11 e 15.

Por fim é inevitável destacar que, mesmo que, por hipótese, fosse possível comprovar a efetiva origem dos documentos eletrônicos “Documento A” e “Documento B” como impressos pelos supostos softwares mencionados pelos colaboradores (denominados “Bankdrop” e “ST”), ainda assim eles não constituiriam uma prova válida.

Isso porque a relevância destes documentos como eventuais provas deriva, de fato, das informações e dos dados neles representados os quais, por sua vez, estariam armazenados e administrados pelos mencionados softwares.

No caso em foco, não é possível separar conceitualmente os softwares dos dados que os mesmos administram. Inclusive podem existir versões diferentes dos softwares e dos dados, com mais ou menos funcionalidades e com mais ou menos informações (como detalhado na resposta ao Quesito 8).

O conjunto de um determinado software e de seus dados (sistema informático), que supostamente originaram os Documentos A e B, é o que deveria ser objeto de análise e perícia oficial para comprovar sua efetiva origem, sua integridade, a real datação dos dados, a ausência de indícios de edição ou alteração e, mais em geral, a consistência da cadeia de custódia.

Ocorre que, pelo que foi possível extrair do HD fornecido pela serventia da Vara, dos documentos disponíveis e dos autos do processo em foco, diversamente do indicado pelo nobre Juízo, em sua decisão de 15/06/2018 (fls. 4681), os colaboradores não entregaram o “sistema Bankdrop” nem qualquer outro sistema, o que impede a realização da necessária perícia.

De fato, ao que se depreende dos autos analisados neste trabalho, os colaboradores somente entregaram documentos em diversos formatos eletrônicos (PDF, TXT, XLS, DOC, JPG, PNG), mas nenhum sistema nem qualquer base de dados que possa ser parte de um sistema.

Oportuno, neste momento, lembrar o que se entende por **sistema** e qual sua diferença em relação a um **simples documento**, o que pode ser auferido pelas definições expressas nos parágrafos iniciais do presente ponto 3 (“Análises e Respostas”).

Neste sentido é mister considerar que estes supostos softwares, ao que se pode deduzir pelas telas capturadas, **preveriam a possibilidade de editar livremente** os dados por eles administrados (ver detalhe 1 na Fig. 19), além de inserir novos dados (detalhe 4 na Fig. 19), esconder a visualização de dados (detalhe 3 na Fig. 19) e cancelar informações (detalhe 2 na Fig. 19).

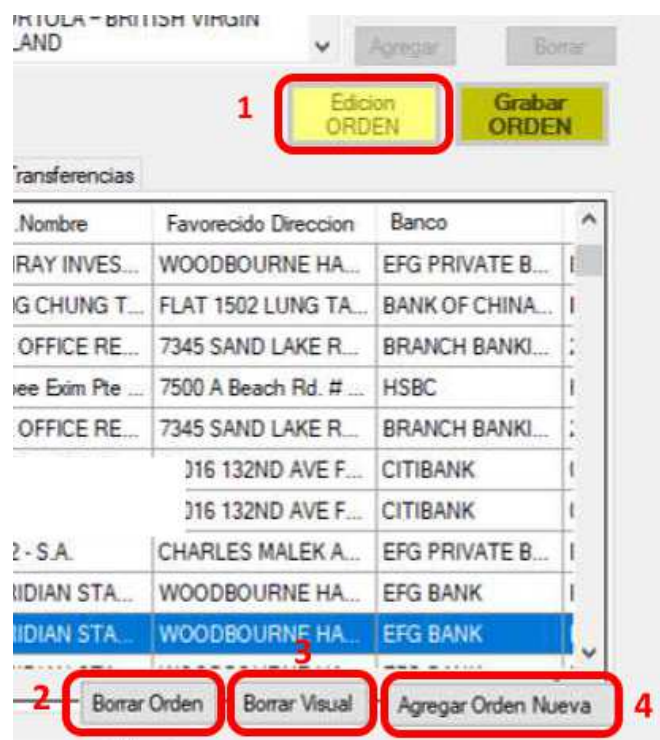


Figura 19

É necessário considerar, ainda, que há nos Documentos A e B, representação de dados que possuem fundamental e crítica importância, quais datas (oportuno lembrar da possível aplicabilidade do instituto da prescrição), valores, nomes e outro detalhes. Estes todos, por óbvio, também editáveis livremente.

Para que estes documentos possam ser considerados como uma prova válida, deveria, por reflexo, ser comprovado, através de uma necessária perícia oficial, que os dados utilizados pelos supostos softwares não foram editados em algum momento (coisa que poderia ter ocorrido pelas mais diversas razões, em qualquer data, por mão de seja quem tivesse acesso aos supostos softwares) e que foram de fato criados originalmente, em sua forma atual, sem posteriores alterações e nas supostas datas apresentadas nos documentos.

Ou seja, seria indispensável comprovar a **real origem, datação e integridade de todos os dados** utilizados pelos supostos softwares, em suma, a consistência da origem e da inteira cadeia de custódia de tais dados.

É inevitável observar que uma colaboração premiada, para ser aceita e válida, e produzir benefícios em favor dos colaboradores, precisa ser suportada por provas.

Esta é, fatalmente, uma, entre várias outras excelentes razões, para produzir falsos vestígios, que possam ser passados por “provas” (mesmo não o sendo, por não poderem ser validadas de qualquer forma confiável), e conseguir, assim, gozar dos benefícios da colaboração.

Por tudo quanto acima entendo que, **no estado atual**, os documentos eletrônicos presentes nos autos, e descritos acima como Documento A e Documento B, certamente **não podem ser considerados provas válidas em um processo penal** (e sequer em um eventual, menos crítico, processo cível).

Para que isso possa ocorrer, deverá **antes** ser realizada uma abrangente perícia oficial em relação a tais documentos, comprovando além de sua autenticidade, sua origem (e a consequente inteira cadeia de custódia) assim como a integridade dos dados e sistema informáticos a partir dos quais foram supostamente criados, entre outros aspectos.

- **Resposta ao Quesito 17.**

Como já exposto na resposta ao Quesito 1, a resposta a esse Quesito precisa de ressalva quanto a possíveis erros, considerado o enorme número e variedade de arquivos presentes no HD em foco.

Através da análise automatizada que foi realizada nos documentos e imagens presentes no HD entregue à defesa, não foi possível localizar o nome da [REDACTED] [REDACTED] relacionado a qualquer documento no qual fosse mencionado o apelido “CABRAL”.

Pela leitura dos autos parece evidente que a associação do apelido “CABRAL” com o nome da [REDACTED], se deu exclusivamente por consequência de declarações dos colaboradores, não acompanhadas de qualquer documento probatório.

4 - Conclusões

Encerrados os trabalhos, conforme acima descritos, respondemos assim aos quesitos postos.

Esperamos ter explorado e trazido aos interessados às informações técnicas, fáticas e jurídicas necessárias, para convicção das partes e do MM. Juízo, e colocamo-nos à inteira disposição para outros esclarecimentos julgados pertinentes.

Nada mais havendo a considerar, damos por encerrado o presente Laudo Técnico, constituído de 31 (trinta e uma) folhas numeradas de 1 a 31, de um só lado, redigidas pelo perito Lorenzo Parodi que subscreve e assina.

Sem mais.

São Paulo, 16 de julho de 2018



Lorenzo Parodi