

LAUDO PERICIAL

Data: 30 de dezembro de 2020

Requerente: *First Responder* Prof. Marcos José Alves de Barros Monteiro

Peritos do Grupo 5:

Jean Abreu da Silva

Karina Costa Ferreira

Márcio Roberto Taglioni dos Santos

Mario Sérgio Filho

Renan Marin de Souza

Rita de Cássia Lima Coelho

Vanessa Rodrigues e Almeida

Data de entrega: 3 de janeiro de 2021

Sumário

1. INTRODUÇÃO	3
2. METODOLOGIA	3
3. FERRAMENTAS UTILIZADAS	3
4. MATERIAL RECEBIDO	5
5. RESPOSTAS AOS QUESITOS.....	7
5.1. Queira o sr perito informar qual sistema operacional e data de instalação do computador coletado	7
5.2. Queira o sr perito informar os softwares instalados e versão dos mesmos no computador coletado e se possível a data de instalação.....	7
5.3. Queira o sr perito informar última vez que o computador coletado foi desligado	9
5.4. Queira o sr perito informar a última vez que o(s) usuário(s) fez(eram) login no computador coletado	9
5.5. Queira o sr perito identificar se há indícios de armazenamento indevido ou quaisquer ofertas ou envio por qualquer meio eletrônico da fórmula secreta a partir do computador coletado.....	10
5.6. Queira o sr perito identificar se, positivo algum item anterior, como este vazamento de dados foi feito no computador coletado	12
5.7. Queira o sr perito identificar se o suspeito teve acesso em algum momento a "Pasta_Proibida" do Servidor	12
5.8. Queira o sr perito identificar se há indícios do crime de pornografia infantil, tanto de armazenamento como de envio no computador coletado.....	14
5.9. Queira o sr perito identificar se há indícios da prática de <i>Fake News</i> no computador coletado	16
5.10. Queira o sr perito identificar se há indícios de um possível planejamento para a prática de homicídio	17
6. CONCLUSÃO	19

1. INTRODUÇÃO

O caso em estudo visa apurar crimes ocorridos na multinacional Full Tummy Food (FTF) pelo USUÁRIO PILANTRA. A denúncia evidencia supostas práticas indevidas de pedofilia, difamação, *Fake News*, roubo e divulgação da “Fórmula Secreta” e planejamento para matar um dos diretores da empresa.

Em razão da necessidade de identificar as possíveis irregularidades, foi contratado um investigador forense que procedeu com a coleta do computador (que continha dois discos rígidos) do USUÁRIO PILANTRA e todo procedimento de cópia forense procedeu com o devido registro da Ata Notarial, com a presença de um tabelião.

Após terminada a fase de coleta e a nomeação dos peritos, foi solicitado um trabalho de análise pericial em equipe no conteúdo dos discos rígidos, com o fito de identificar materialidade, autoria e se possível culpabilidade das ações supracitadas, respondendo alguns quesitos através de Laudo Pericial.

O objetivo desse Laudo Pericial é apresentar as irregularidades identificadas, na análise, no atendimento aos dez quesitos relacionados no documento “AVALIAÇÃO.DOC”, disponibilizado no Portal do Aluno do sítio do Instituto de Pós-graduação e Graduação – IPOG.

2. METODOLOGIA

A metodologia de análise forense utilizada foi a *Post Mortem*, na qual somente os dados não voláteis podem ser objeto de análise.

Na análise *Post Mortem*, foram utilizadas ferramentas livres para a realização dos exames forenses nos dispositivos de armazenamento de dados.

3. FERRAMENTAS UTILIZADAS

Os *softwares* utilizados na perícia foram o AccessData® FTK® Imager 4.3.1.1 (FIGURA 1), o Rip v.2.8_20200220 - CLI RegRipper tool (FIGURA2), SPLView e Browsing History View versão v2.40.



FIGURA 1 - AccessData® FTK® Imager 4.3.1.1

```
Rip v.2.8_20200220 - CLI RegRipper tool
Rip [-r Reg hive file] [-f plugin file] [-p plugin module] [-l] [-h]
Parse Windows Registry files, using either a single module, or a plugins file.

NOTE: This tool does NOT automatically process Registry transaction logs! The tool
does check to see if the hive is dirty, but does not automatically process the
transaction logs. If you need to incorporate transaction logs, please consider
using yarp + registryFlush.py, or rla.exe from Eric Zimmerman.

-r Reg hive file...Registry hive file to parse
-g .....Guess the hive file (experimental)
-f [profile].....use the plugin file (default: plugins\plugins)
-p plugin module...use only this module
-l .....list all plugins
-c .....Output list in CSV format (use with -l)
-s system name.....Server name (TLN support)
-u username.....User name (TLN support)
-uP .....Update profiles
-h.....Help (print this information)

Ex: C:\>rip -r c:\case\system -f system
    C:\>rip -r c:\case\ntuser.dat -p userassist
    C:\>rip -l -c

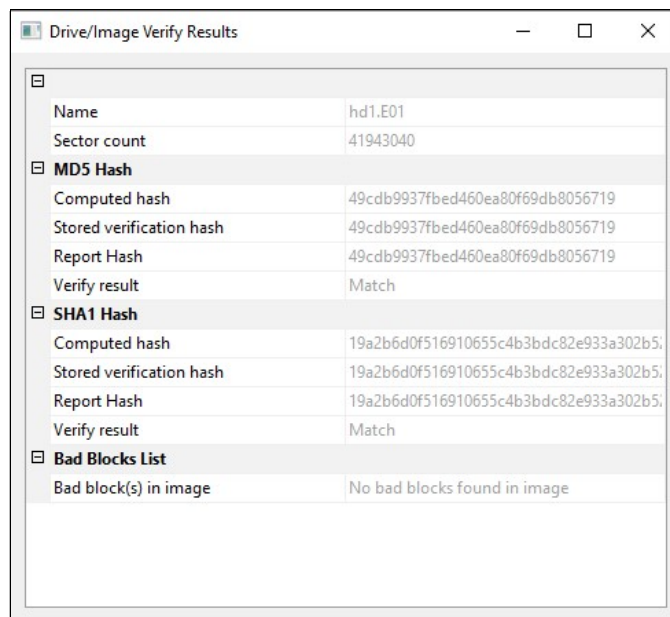
All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.

copyright 2020 Quantum Analytics Research, LLC
```

FIGURA 2 - Rip v.2.8_20200220 - CLI RegRipper tool

4. MATERIAL RECEBIDO

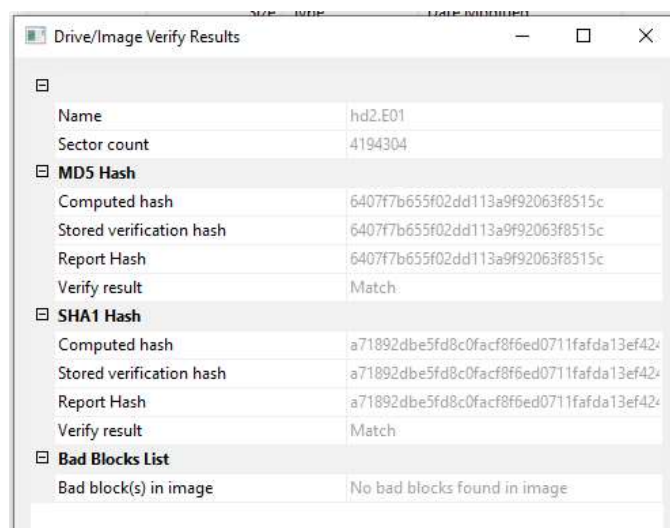
Foram recebidos arquivos com imagens de dois discos rígidos. O primeiro (hd1) com Hash MD5 “49cdb9937fbed460ea80f69db8056719” (FIGURA 3) e o segundo (hd2) com Hash MD5 “6407f7b655f02dd113a9f92063f8515c” (FIGURA 4).



The screenshot shows a window titled "Drive/Image Verify Results" with a table of verification data for "hd1.E01". The table includes fields for Name, Sector count, MD5 Hash (Computed, Stored, Report, and Verify result), SHA1 Hash (Computed, Stored, Report, and Verify result), and Bad Blocks List (Bad block(s) in image).

Drive/Image Verify Results	
Name	hd1.E01
Sector count	41943040
MD5 Hash	
Computed hash	49cdb9937fbed460ea80f69db8056719
Stored verification hash	49cdb9937fbed460ea80f69db8056719
Report Hash	49cdb9937fbed460ea80f69db8056719
Verify result	Match
SHA1 Hash	
Computed hash	19a2b6d0f516910655c4b3bdc82e933a302b5;
Stored verification hash	19a2b6d0f516910655c4b3bdc82e933a302b5;
Report Hash	19a2b6d0f516910655c4b3bdc82e933a302b5;
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

FIGURA 3 - Tamanho do hd1



The screenshot shows a window titled "Drive/Image Verify Results" with a table of verification data for "hd2.E01". The table includes fields for Name, Sector count, MD5 Hash (Computed, Stored, Report, and Verify result), SHA1 Hash (Computed, Stored, Report, and Verify result), and Bad Blocks List (Bad block(s) in image).

Drive/Image Verify Results	
Name	hd2.E01
Sector count	4194304
MD5 Hash	
Computed hash	6407f7b655f02dd113a9f92063f8515c
Stored verification hash	6407f7b655f02dd113a9f92063f8515c
Report Hash	6407f7b655f02dd113a9f92063f8515c
Verify result	Match
SHA1 Hash	
Computed hash	a71892dbe5fd8c0facf8f6ed0711fafda13ef42;
Stored verification hash	a71892dbe5fd8c0facf8f6ed0711fafda13ef42;
Report Hash	a71892dbe5fd8c0facf8f6ed0711fafda13ef42;
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

FIGURA 4 - Tamanho do hd2

Foi realizada uma cópia integral dos conteúdos das imagens dos dois discos rígidos recebidos. A montagem das imagens no FTK Imager é apresentada na FIGURA 5, conforme abaixo.

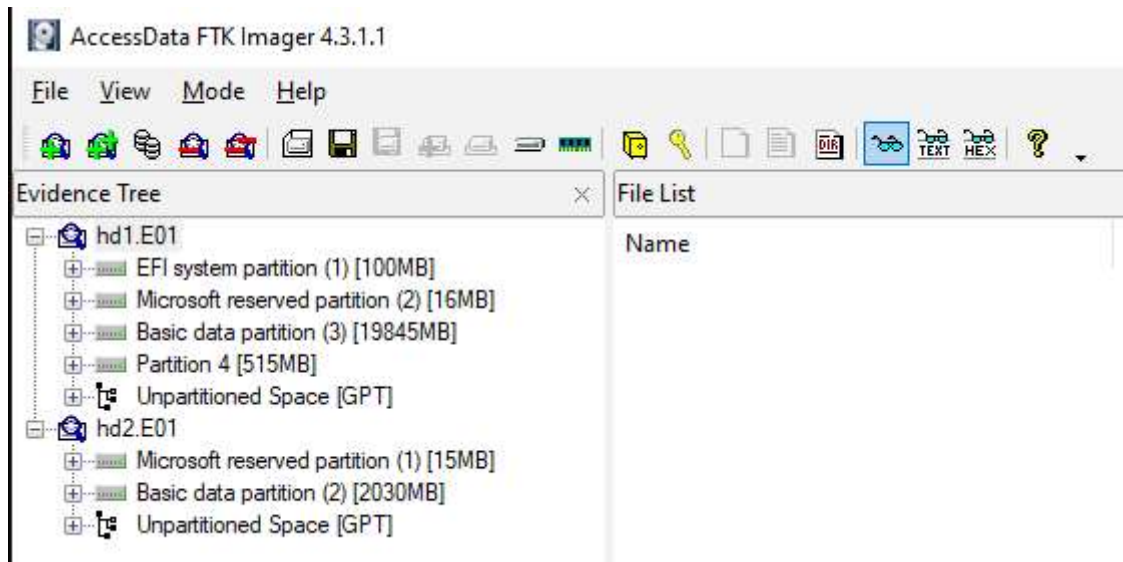


FIGURA 5 - Montagem dos discos rígidos

5. RESPOSTAS AOS QUESITOS

5.1. Queira o sr perito informar qual sistema operacional e data de instalação do computador coletado

Resposta: O sistema operacional do computador coletado é o Windows 10 Pro e a data de instalação é 11 de junho de 2020.

Para obter a informação, foi utilizado a ferramenta rip e o comando utilizado foi o “rip -r \ANALISE\SOFTWARE -p winver”, conforme FIGURA 6.

```
C:\RR>rip -r \ANALISE\SOFTWARE -p winver
***Hive Check***
The hive (\ANALISE\SOFTWARE) is dirty.
Please consider processing hive transaction logs via either Maxim's yarp + registryFlush.py
or via Eric Zimmerman's rla.exe.

Launching winver v.20081210
winver v.20081210
(Software) Get Windows version

ProductName = Windows 10 Pro
InstallDate = Thu Jun 11 19:49:05 2020
```

FIGURA 6 - Identificação do sistema operacional

5.2. Queira o sr perito informar os softwares instalados e versão dos mesmos no computador coletado e se possível a data de instalação

Resposta: Foram encontrados 34 *softwares* no computador coletado, conforme FIGURA 7.

Para obter a informação, foi utilizada a ferramenta rip e os comandos foram: “RR>rip -r \ANALISE\SOFTWARE -p uninstall” e “rip -r \Analise\Software -p uninstall_tln”, conforme FIGURA 8.

	SOFTWARE	DATA DE INSTALAÇÃO		SOFTWARE	DATA DE INSTALAÇÃO
1	LibreOffice 6.4.4.2	Mon Jun 15 21:13:25 2020 (UTC)	18	eMule	Mon Jun 15 21:26:35 2020 (UTC)
2	Mozilla Maintenance Service	Mon Jun 15 21:07:28 2020 (UTC)	19	Google Update Helper	Mon Jun 15 21:11:24 2020 (UTC)
3	DXM_Runtime	Sat Dec 7 14:56:36 2019 (UTC)	20	Mozilla Firefox 77.0.1	Mon Jun 15 21:07:28 2020 (UTC)
4	MPlayer2	Sat Dec 7 14:56:36 2019 (UTC)	21	Google Chrome	Mon Jun 15 21:06:36 2020 (UTC)

5	AddressBook	Sat Dec 7 09:17:28 2019 (UTC)	22	DXM_Runtime	Sat Dec 7 14:56:36 2019 (UTC)
6	Connection Manager	Sat Dec 7 09:17:28 2019 (UTC)	23	MPlayer2	Sat Dec 7 14:56:36 2019 (UTC)
7	DirectDrawEx	Sat Dec 7 09:17:28 2019 (UTC)	24	AddressBook	Sat Dec 7 09:17:27 2019 (UTC)
8	Fontcore	Sat Dec 7 09:17:28 2019 (UTC)	25	Connection Manager	Sat Dec 7 09:17:27 2019 (UTC)
9	IE40	Sat Dec 7 09:17:28 2019 (UTC)	26	DirectDrawEx	Sat Dec 7 09:17:27 2019 (UTC)
10	IE4Data	Sat Dec 7 09:17:28 2019 (UTC)	27	Fontcore	Sat Dec 7 09:17:27 2019 (UTC)
11	IE5BAKEX	Sat Dec 7 09:17:28 2019 (UTC)	28	IE40	Sat Dec 7 09:17:27 2019 (UTC)
12	IEData	Sat Dec 7 09:17:28 2019 (UTC)	29	IE4Data	Sat Dec 7 09:17:27 2019 (UTC)
13	MobileOptionPack	Sat Dec 7 09:17:28 2019 (UTC)	30	IE5BAKEX	Sat Dec 7 09:17:27 2019 (UTC)
14	SchedulingAgent	Sat Dec 7 09:17:28 2019 (UTC)	31	IEData	Sat Dec 7 09:17:27 2019 (UTC)
15	WIC	Sat Dec 7 09:17:28 2019 (UTC)	32	MobileOptionPack	Sat Dec 7 09:17:27 2019 (UTC)
16	Adobe Acrobat Reader DC	Mon Jun 15 21:52:58 2020 (UTC)	33	SchedulingAgent	Sat Dec 7 09:17:27 2019 (UTC)
17	Adobe Refresh Manager	Mon Jun 15 21:52:28 2020 (UTC)	34	WIC	Sat Dec 7 09:17:27 2019 (UTC)

FIGURA 7 - Lista de softwares encontrados

```

C:\RR>rip -r \Analise\Software -p uninstall_tln
***Hive Check***
The hive (\Analise\Software) is dirty.
Please consider processing hive transaction logs via either Maxim's yarp + registryFlush.py
or via Eric Zimmerman's rla.exe.

Launching uninstall v.20120523
Uninstall
Microsoft\Windows\CurrentVersion\Uninstall

1592255605|REG|[Uninstall] - LibreOffice 6.4.4.2 v.6.4.4.2
1592255248|REG|[Uninstall] - Mozilla Maintenance Service v.77.0.1
1575730596|REG|[Uninstall] - DXM_Runtime
1575730596|REG|[Uninstall] - MPlayer2
1575710248|REG|[Uninstall] - AddressBook
1575710248|REG|[Uninstall] - Connection Manager
1575710248|REG|[Uninstall] - DirectDrawEx
1575710248|REG|[Uninstall] - Fontcore
1575710248|REG|[Uninstall] - IE40
1575710248|REG|[Uninstall] - IE4Data
1575710248|REG|[Uninstall] - IE5BAKEX
1575710248|REG|[Uninstall] - IEData
1575710248|REG|[Uninstall] - MobileOptionPack
1575710248|REG|[Uninstall] - SchedulingAgent
1575710248|REG|[Uninstall] - WIC
Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

1592257978|REG|[Uninstall] - Adobe Acrobat Reader DC - Portuguese v.19.010.20098
1592257948|REG|[Uninstall] - Adobe Refresh Manager v.1.8.0
1592256395|REG|[Uninstall] - eMule
1592255484|REG|[Uninstall] - Google Update Helper v.1.3.35.451
1592255248|REG|[Uninstall] - Mozilla Firefox 77.0.1 (x86 pt-BR) v.77.0.1
1592255196|REG|[Uninstall] - Google Chrome v.83.0.4103.106
1575730596|REG|[Uninstall] - DXM_Runtime
1575730596|REG|[Uninstall] - MPlayer2
1575710247|REG|[Uninstall] - AddressBook
1575710247|REG|[Uninstall] - Connection Manager
1575710247|REG|[Uninstall] - DirectDrawEx
1575710247|REG|[Uninstall] - Fontcore
1575710247|REG|[Uninstall] - IE40
1575710247|REG|[Uninstall] - IE4Data
1575710247|REG|[Uninstall] - IE5BAKEX
1575710247|REG|[Uninstall] - IEData
1575710247|REG|[Uninstall] - MobileOptionPack
1575710247|REG|[Uninstall] - SchedulingAgent
1575710247|REG|[Uninstall] - WIC

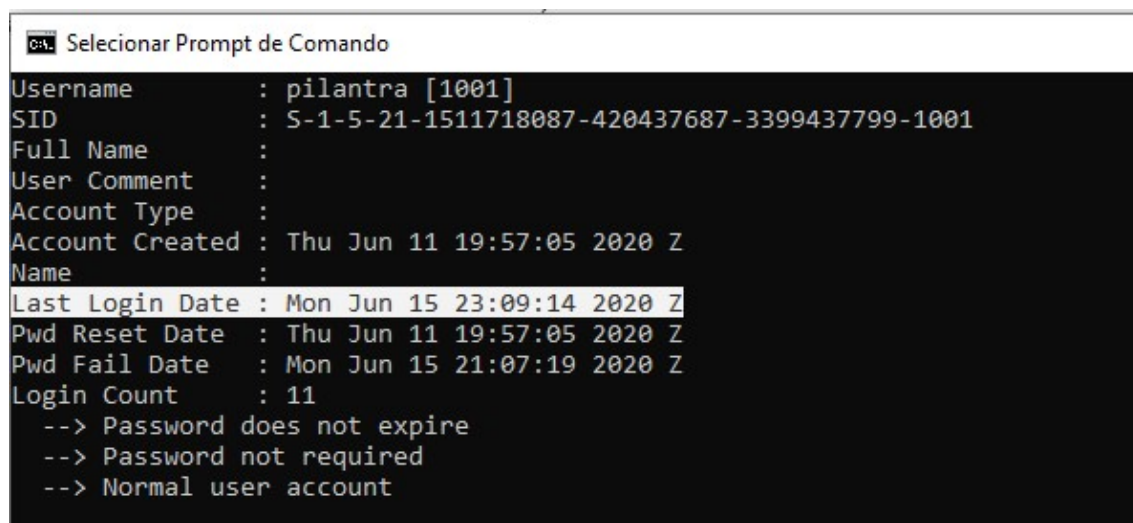
```

FIGURA 8 - Comando rip para listar os softwares

5.3. Queira o sr perito informar última vez que o computador coletado foi desligado

Resposta: A última vez que fizeram login no computador coletado foi em 15 de junho de 2020 as 23:09:14 z.

Para obter a informação, foi utilizada a ferramenta rip, comando “rip -r \Analise\SAM -p samparse”.



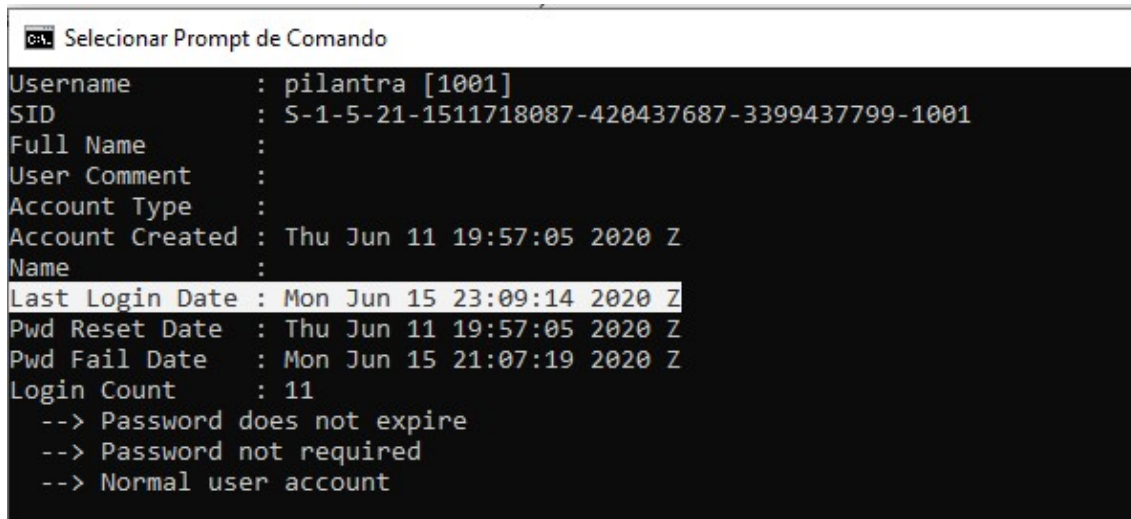
```
Selecionar Prompt de Comando
Username      : pilantra [1001]
SID           : S-1-5-21-1511718087-420437687-3399437799-1001
Full Name     :
User Comment  :
Account Type  :
Account Created : Thu Jun 11 19:57:05 2020 Z
Name          :
Last Login Date : Mon Jun 15 23:09:14 2020 Z
Pwd Reset Date : Thu Jun 11 19:57:05 2020 Z
Pwd Fail Date  : Mon Jun 15 21:07:19 2020 Z
Login Count    : 11
--> Password does not expire
--> Password not required
--> Normal user account
```

FIGURA 9 – Última vez que o computador foi desligado

5.4. Queira o sr perito informar a última vez que o(s) usuário(s) fez(eram) login no computador coletado

Resposta: A última vez que fizeram login no computador coletado foi em 15 de junho de 2020 as 23:09:14 z.

Para obter a informação, foi utilizada a ferramenta rip, comando “rip -r \Analise\SAM -p samparse”.



```
cmd Selecionar Prompt de Comando
Username      : pilantra [1001]
SID           : S-1-5-21-1511718087-420437687-3399437799-1001
Full Name     :
User Comment  :
Account Type  :
Account Created : Thu Jun 11 19:57:05 2020 Z
Name          :
Last Login Date : Mon Jun 15 23:09:14 2020 Z
Pwd Reset Date : Thu Jun 11 19:57:05 2020 Z
Pwd Fail Date  : Mon Jun 15 21:07:19 2020 Z
Login Count    : 11
--> Password does not expire
--> Password not required
--> Normal user account
```

FIGURA 10 - Última vez que o computador foi desligado

5.5. Queira o sr perito identificar se há indícios de armazenamento indevido ou quaisquer ofertas ou envio por qualquer meio eletrônico da fórmula secreta a partir do computador coletado

Resposta parte 1: Foram encontrados indícios de armazenamento indevido, tais como s00 Martin Nice 12yo Boy With Man.jpg; Boyman27 - great anal sex - cute 6yo little boy and daddy toddler best.png; 11yo.2.boys.anal.1628.bibcam.omegle.2014.jpg; 3 boys 12yo 11yo and 7yo have fun on webcam_05.jpg. Segue a lista de mais arquivos na FIGURA abaixo.

Para obter a informação, foi utilizada a ferramenta rip, comando “rip -r \Analise\NTUSER.DAT -p recentdocs”

Resposta parte 2: Foi identificado uma conversa no Skype do user pilantra, com o possível compartilhamento da fórmula secreta, conforme abaixo.

INSTITUTO DE PÓS-GRADUAÇÃO E GRADUAÇÃO MBA INFORMÁTICA FORENSE MÓDULO ASPECTOS GERAIS DA INFORMÁTICA FORENSE APLICADA

```
C:\WINDOWS\system32\cmd.exe
- Correlate the user SIDs to the output of the ProfileList plugin

C:\RR>rip -r \Analis\NTUSER.DAT -p recentdocs
***Hive Check***
The hive (\Analis\NTUSER.DAT) is dirty.
Please consider processing hive transaction logs via either Maxim's yarp + registryFlush.py
or via Eric Zimmerman's rla.exe.

Launching recentdocs v.20100405
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Mon Jun 15 23:23:39 2020 (UTC)
21 = MPMEN (D:)
46 = Chave de Recuperaç[...]\João do BitLocker AF23B6DB-45D2-4CB1-A8BB-ASAB14A3FBAE.TXT
36 = XXXX
37 = s00 Martin Nice 12yo Boy With Man.jpg
40 = Boyman27 - great anal sex - cute oyo little boy and daddy toddler best.png
41 = download.jpg
42 = Bibcam Webcam - smooth hung 13yo teen boy jerks with fleshlight 25-May-2014 pthc xcam.jpg
43 = 11yo.2.boys.anal.1628.bibcam.omegle.2014.jpg
47 = 8yo + 9 yo + man Bibcam Omele 2012.04.30 [boy+man] 3 Swedish Ver1 Cute Boys 7yo 9yo 10yo With Man).mpg.jpg
45 = Downloads
44 = 822eb55acc6f06047592d093a2610b0.jpg
6 = PASTA PROIBIDA
9 = Formula Secreta.docx
32 = Applications
31 = Microsoft.Windows.Computer
43 = pthc
2 = Sistema e Segurança
1 = ::{BB86C8E4-D293-4F75-8A90-CB05B6477EEE}
38 = Pretten Nude Naked Pedo best.jpg
35 = 3 boys 12yo 11yo and 7yo have fun on webcam_05.jpg
34 = Internet
33 = search?q=chumbinho+matas&elv=AXXfrEiqD9r3GueIwApulP0bAolZL3r8d9j4olredHIT1Y5qUEf3hzmUsStqVdLleV*3TDHtWdngE!Cvp*xrNseitApaHqk3cwcAs9j
30 = Contrabilidade.odt
29 = Palestra SP - Agosto2019
28 = Palestra CSI - 2 pra direito .odp
27 = MM-PLUS (D:)
23 = Disco Local (C:)
```

FIGURA 11 - Indícios de armazenamento indevido

	creator	compose_time	msg_content	original_arrival_time
1	8:live:cid.6413a4160701880e	2020-06-15T21:33:47.025Z	<ss type="hi">(wave)</ss>	2020-06-15T21:33:47.025Z
2	8:marcosmonteiro.com.br	2020-06-15T21:47:54.177Z	<URIObject uri="https://api.asm.skype.com/v1/objects/0-eus-...	2020-06-15T21:47:54.177Z
3	8:live:cid.6413a4160701880e	2020-06-15T21:46:21.689Z	manda	2020-06-15T21:46:21.689Z
4	8:marcosmonteiro.com.br	2020-06-15T21:44:23.972Z	CPF da geral !!	2020-06-15T21:44:23.972Z
5	8:marcosmonteiro.com.br	2020-06-15T21:44:10.598Z	Te falei q to com umas infos ?	2020-06-15T21:44:10.598Z
6	8:marcosmonteiro.com.br	2020-06-15T21:43:44.977Z	Filet !!!!	2020-06-15T21:43:44.977Z
7	8:live:cid.6413a4160701880e	2020-06-15T21:43:35.922Z	mandei	2020-06-15T21:43:35.922Z
8	8:live:cid.6413a4160701880e	2020-06-15T21:43:27.892Z	<URIObject uri="https://api.asm.skype.com/v1/objects/0-eus-d2-...	2020-06-15T21:43:27.892Z
9	8:live:cid.6413a4160701880e	2020-06-15T21:43:00.516Z	tu é p bichão mermo!!	2020-06-15T21:43:00.516Z
10	8:live:cid.6413a4160701880e	2020-06-15T21:42:44.281Z	showWWW	2020-06-15T21:42:44.281Z
11	8:marcosmonteiro.com.br	2020-06-15T21:42:34.985Z	3E6UEJpyCQp4YTczMQj4vS6qqYcn9sRSIE	2020-06-15T21:42:34.985Z
12	8:marcosmonteiro.com.br	2020-06-15T21:41:37.434Z	Se liga	2020-06-15T21:41:37.434Z
13	8:marcosmonteiro.com.br	2020-06-15T21:41:35.428Z	É uma parada	2020-06-15T21:41:35.428Z
14	8:live:cid.6413a4160701880e	2020-06-15T21:41:24.359Z	como assim?	2020-06-15T21:41:24.359Z
15	8:marcosmonteiro.com.br	2020-06-15T21:41:08.009Z	Já já chega pra ti de uma carteira q tenho aqui	2020-06-15T21:41:08.009Z
16	8:marcosmonteiro.com.br	2020-06-15T21:40:55.865Z	Vou mandar pra ti então	2020-06-15T21:40:55.865Z
17	8:live:cid.6413a4160701880e	2020-06-15T21:40:33.186Z	pode ser bitcoin, ta ligado?	2020-06-15T21:40:33.186Z
18	8:marcosmonteiro.com.br	2020-06-15T21:40:24.060Z	Tu quer como ?	2020-06-15T21:40:24.060Z
19	8:marcosmonteiro.com.br	2020-06-15T21:40:07.436Z	Caramba moleque, assim vc me quebra	2020-06-15T21:40:07.436Z
20	8:live:cid.6413a4160701880e	2020-06-15T21:39:49.373Z	manda R\$ 150.000,00, aproveita a promoção	2020-06-15T21:39:49.373Z
21	8:live:cid.6413a4160701880e	2020-06-15T21:39:22.138Z	seguite	2020-06-15T21:39:22.138Z
22	8:marcosmonteiro.com.br	2020-06-15T21:39:14.419Z	Fala quanto	2020-06-15T21:39:14.419Z
23	8:live:cid.6413a4160701880e	2020-06-15T21:39:09.091Z	a gente paga como o leite dos guris?	2020-06-15T21:39:09.091Z
24	8:live:cid.6413a4160701880e	2020-06-15T21:38:57.060Z	tem q molhar a mao	2020-06-15T21:38:57.060Z

25	8:live::cid.6413a4160701880e	2020-06-15T21:38:53.279Z	ne assim não mano	2020-06-15T21:38:53.279Z
26	8:marcosmonteiro.com.br	2020-06-15T21:38:45.574Z	Manda	2020-06-15T21:38:45.574Z
27	8:marcosmonteiro.com.br	2020-06-15T21:38:40.601Z	Quero	2020-06-15T21:38:40.601Z
28	8:marcosmonteiro.com.br	2020-06-15T21:38:37.800Z	Filet	2020-06-15T21:38:37.800Z
29	8:live::cid.6413a4160701880e	2020-06-15T21:38:19.544Z	interessa?	2020-06-15T21:38:19.544Z
30	8:live::cid.6413a4160701880e	2020-06-15T21:38:16.966Z	te intererrsa?	2020-06-15T21:38:16.966Z
31	8:live::cid.6413a4160701880e	2020-06-15T21:38:11.544Z	diz ai	2020-06-15T21:38:11.544Z
32	8:live::cid.6413a4160701880e	2020-06-15T21:38:07.204Z	<URIObject uri="https://api.asm.skype.com/v1/objects/0-eus-...	2020-06-15T21:38:07.204Z
33	8:live::cid.6413a4160701880e	2020-06-15T21:37:49.950Z	só pra tu pirar, ta ligado?	2020-06-15T21:37:49.950Z
34	8:live::cid.6413a4160701880e	2020-06-15T21:37:39.153Z	vou te mandar uma parte so	2020-06-15T21:37:39.153Z
35	8:live::cid.6413a4160701880e	2020-06-15T21:36:03.199Z	ta ligado?	2020-06-15T21:36:03.199Z
36	8:live::cid.6413a4160701880e	2020-06-15T21:36:00.637Z	um lance de doido pra nois ficar rico	2020-06-15T21:36:00.637Z
37	8:live::cid.6413a4160701880e	2020-06-15T21:35:50.215Z	se lembra q te falei de uma formula secreta?	2020-06-15T21:35:50.215Z
38	8:live::cid.6413a4160701880e	2020-06-15T21:35:41.136Z	diz ai	2020-06-15T21:35:41.136Z
39	8:marcosmonteiro.com.br	2020-06-15T21:35:29.262Z	Sóooooo	2020-06-15T21:35:29.262Z
40	8:live::cid.6413a4160701880e	2020-06-15T21:35:14.746Z	é noooois, ta ligado?	2020-06-15T21:35:14.746Z
41	8:marcosmonteiro.com.br	2020-06-15T21:34:56.032Z	O bagulho é doido !	2020-06-15T21:34:56.032Z
42	8:live::cid.6413a4160701880e	2020-06-15T21:34:41.261Z	ta ligado na parada?	2020-06-15T21:34:41.261Z
43	8:live::cid.6413a4160701880e	2020-06-15T21:34:35.761Z	mó li li	2020-06-15T21:34:35.761Z
44	8:marcosmonteiro.com.br	2020-06-15T21:34:24.842Z	E tu? Como tatu ?	2020-06-15T21:34:24.842Z
45	8:marcosmonteiro.com.br	2020-06-15T21:34:18.185Z	Na Nice	2020-06-15T21:34:18.185Z
46	8:marcosmonteiro.com.br	2020-06-15T21:34:13.019Z	Limpeza	2020-06-15T21:34:13.019Z
47	8:live::cid.6413a4160701880e	2020-06-15T21:33:56.432Z	e ai mano, qual a boa de hoje?	2020-06-15T21:33:56.432Z
48	8:live::cid.6413a4160701880e	2020-06-15T21:52:48.380Z	TOP demais	2020-06-15T21:52:48.380Z
49	8:live::cid.6413a4160701880e	2020-06-15T21:52:58.380Z	isso me dá vontade de aprontar muito	2020-06-15T21:52:58.380Z
50	8:marcosmonteiro.com.br	2020-06-15T21:53:25.748Z	SÓ SE FOR DENOVO	2020-06-15T21:53:25.748Z
51	8:marcosmonteiro.com.br	2020-06-15T21:53:35.795Z	TU É MUITO PILANTRA VE!!!	2020-06-15T21:53:35.795Z
52	8:live::cid.6413a4160701880e	2020-06-15T21:53:43.803Z	É NOIS!!!!	2020-06-15T21:53:43.803Z
53	8:live::cid.6413a4160701880e	2020-06-15T21:54:08.053Z	ei, já me vou, vou mi já!	2020-06-15T21:54:08.053Z
54	8:marcosmonteiro.com.br	2020-06-15T21:54:13.717Z	FALOU VEI	2020-06-15T21:54:13.717Z

FIGURA 12 - Possível compartilhamento da fórmula secreta

5.6. Queira o sr perito identificar se, positivo algum item anterior, como este vazamento de dados foi feito no computador coletado

Resposta: O possível vazamento da fórmula secreta pode ter sido realizado por meio do aplicativo Skype, conforme conversa da FIGURA 12.

5.7. Queira o sr perito identificar se o suspeito teve acesso em algum momento a "Pasta_Proibida" do Servidor

Resposta: Foi identificado que o suspeito acessou o arquivo Pasta_Proibida em 15/06/2020.

Para a verificação do arquivo acessado recentemente, foi utilizada a ferramenta rip com o comando: “rip -r \Analise\NTUSER.DAT -p recentdocs_timeline” e “rip -r \analise\ntuser.dat -p ntusernetwork”. Abaixo índice de salvamento em PNG, pilantra/pictures/semtitulo.png.


```

C:\Users\user> VAnalyzeNTUSER.DAT -p recentdocs_timeline
***Hive Check***
The hive (VAnalyzeNTUSER.DAT) is dirty.
Please consider processing hive transaction logs via either Maxim's yarp + registryFlush.py
or via Eric Zimmerman's rla.exe.

Launching recentdocs_timeline v.20161112
recentdocs_timeline v.20161112
(NTUSER.DAT) Gets contents of user's RecentDocs key and place last write times into timeline based on MRUListEx

RecentDocs
Thu Jun 11 19:57:59 2020      : NO VALUES - CHECK KEY MANUALLY
Mon Jun 15 23:09:32 2020      : Microsoft.Windows.Computer
Mon Jun 15 23:11:36 2020      : Formula_Secreta.docx
Mon Jun 15 23:23:33 2020      : s00 Martin Nice 12yo Boy With Man.jpg
Mon Jun 15 22:36:16 2020      : Palestra CSI - 2 pra direito .odp
Mon Jun 15 22:38:40 2020      : Cotnabilidade.odt
Mon Jun 15 22:27:43 2020      : AULA1FCOEBI.pdf
Mon Jun 15 23:23:31 2020      : Boyman27 - great anal sex - cute 6yo little boy and daddy toddler best.png
Mon Jun 15 23:23:39 2020      : Chave de Recupera[?]ão do BitLocker AF2386DB-45D2-4C01-A0BB-A5A014A3FBAE.TXT
Mon Jun 15 23:23:39 2020      : MMPEN (D:)

The last write times are now placed in line with the values in the MRUListEx value
Mon Jun 15 23:23:39 2020      21 = MMPEN (D:)
Mon Jun 15 23:23:39 2020      46 = Chave de Recupera[?]ão do BitLocker AF2386DB-45D2-4C01-A0BB-A5A014A3FBAE.TXT
36 = XXX
Mon Jun 15 23:23:33 2020      37 = s00 Martin Nice 12yo Boy With Man.jpg
Mon Jun 15 23:23:31 2020      40 = Boyman27 - great anal sex - cute 6yo little boy and daddy toddler best.png
39 = download.jpg
41 = Bilibili Webcam - smooth hung 13yo teen boy jerks with fleshlight 25-May-2014 pthc xcam.jpg
42 = 11yo.2.boys.anal.1628.bilibili.omegle.2014.jpg
47 = 8yo + 9 yo + man Bilibili Omele 2012.04.30 [boy+man] 3 Swedish Ver1 Cute Boys 7yo 9yo 10yo With Man).mpg.jpg
45 = Downloads
44 = 862eba55acc6f06047592d893a2610b0.jpg
6 = PASTA_PROIBIDA
Mon Jun 15 23:11:36 2020      0 = Formula_Secreta.docx
32 = Applications
31 = Microsoft.Windows.Computer
43 = pthc
2 = Sistema e Seguran[?]a
1 = {:[BB86C8E4-D293-4F75-BA90-CB05B6477EEE]}
38 = Pretsen Nude Naked Pado best.jpg
35 = 3 boys 12yo 11yo and 7yo have fun on webcam_05.jpg
34 = Internet
  
```

FIGURA 13 – Acesso a pasta proibida

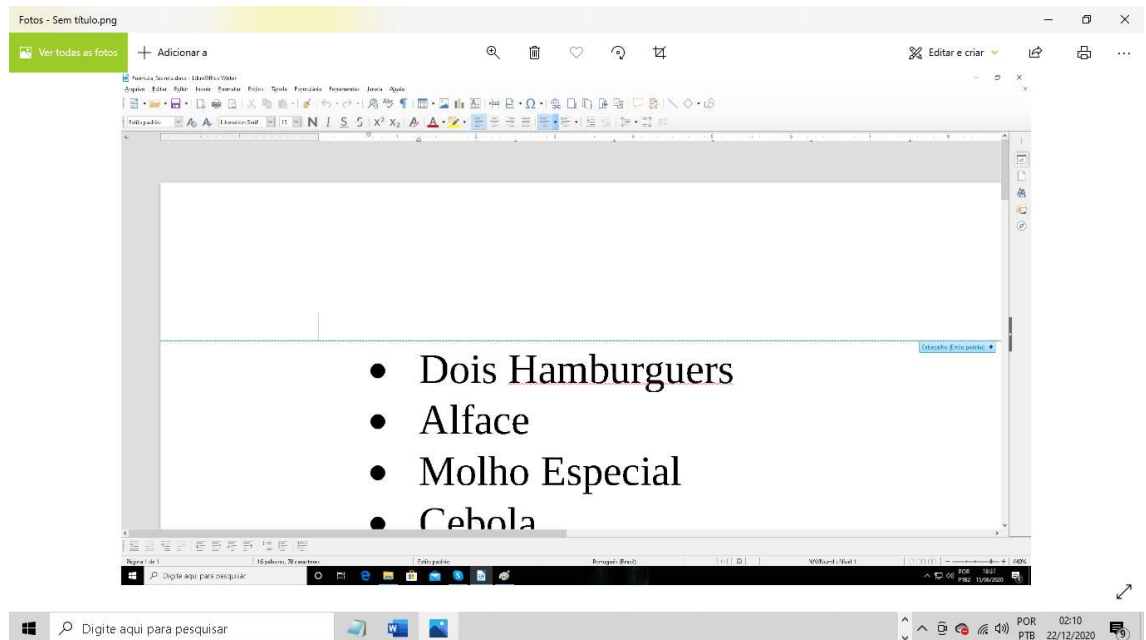


FIGURA 14 – Fórmula Secreta

INSTITUTO DE PÓS-GRADUAÇÃO E GRADUAÇÃO MBA INFORMÁTICA FORENSE MÓDULO ASPECTOS GERAIS DA INFORMÁTICA FORENSE APLICADA

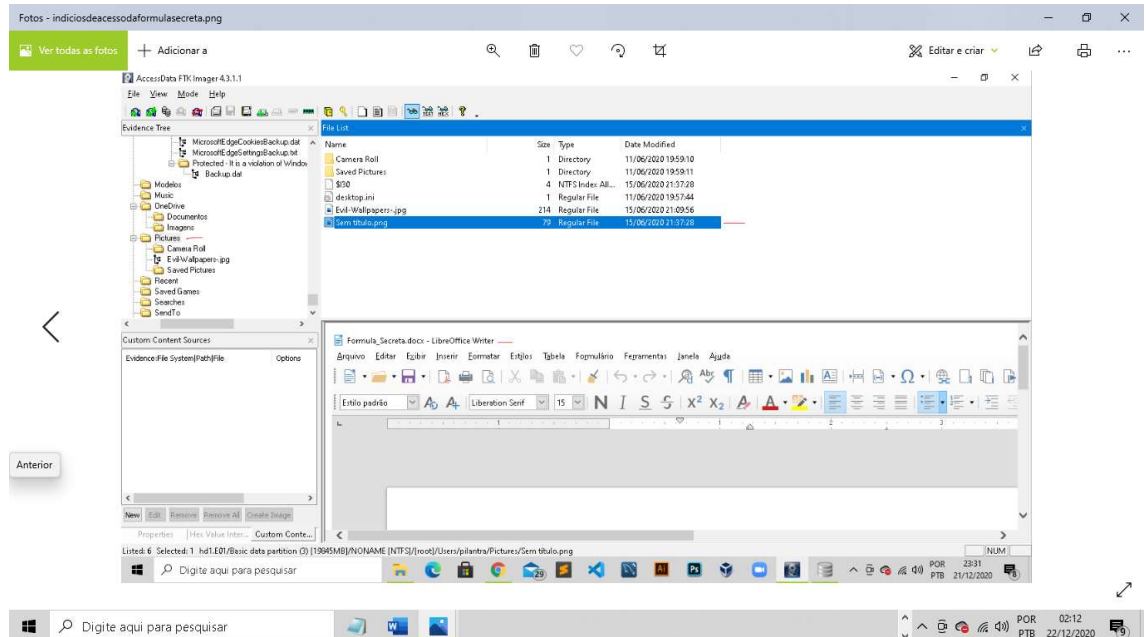


FIGURA 15 – Indícios de acesso a pasta proibida e fórmula secreta

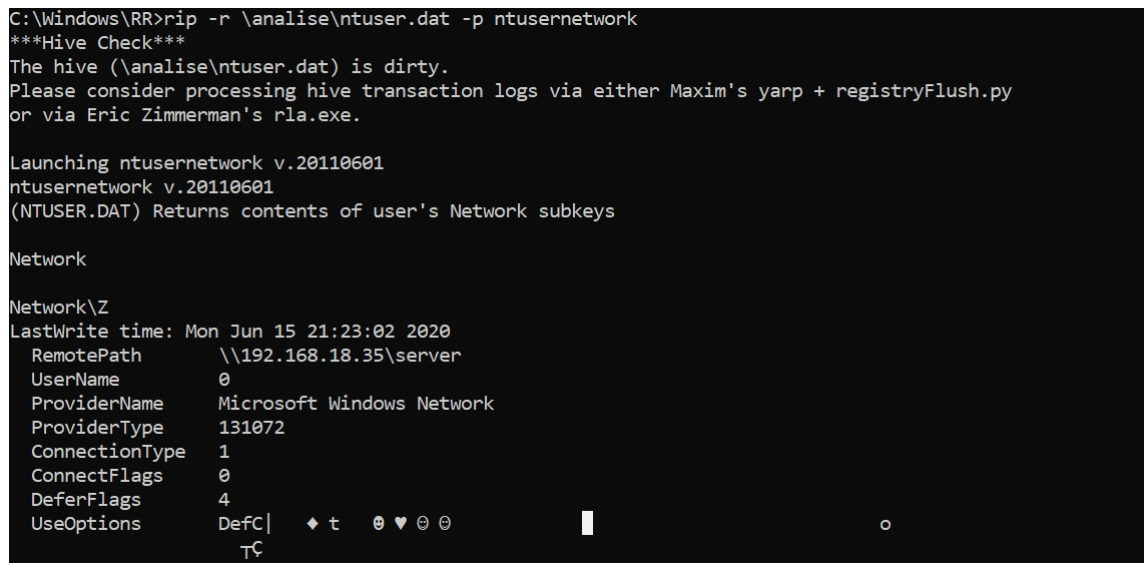


FIGURA 16 - Acesso remoto ao servidor 192.168.18.35

5.8. Queira o sr perito identificar se há indícios do crime de pornografia infantil, tanto de armazenamento como de envio no computador coletado

Resposta: Foi encontrado indícios de crime de pornografia infantil no computador coletado em um arquivo excluído encontrado na lixeira.

INSTITUTO DE PÓS-GRADUAÇÃO E GRADUAÇÃO
MBA INFORMÁTICA FORENSE
MÓDULO ASPECTOS GERAIS DA INFORMÁTICA FORENSE APLICADA
Também foi encontrado acessos de sites pornográficos que apresentam crianças e menor de idade com a utilização da ferramenta Browsing History View.

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	15/06/2020 23:07:22
\$IN7BM23.jpg	1	Regular File	15/06/2020 23:07:07
\$RN7BM23.jpg	10	Regular File	15/06/2020 22:57:28
desktop.ini	1	Regular File	11/06/2020 19:57:48

FIGURA 17 - Indícios de pornografia

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	15/06/2020 23:07:22
\$IN7BM23.jpg	1	Regular File	15/06/2020 23:07:07
\$RN7BM23.jpg	10	Regular File	15/06/2020 22:57:28
desktop.ini	1	Regular File	11/06/2020 19:57:48



FIGURA 18 - Arquivo excluído encontrado na lixeira

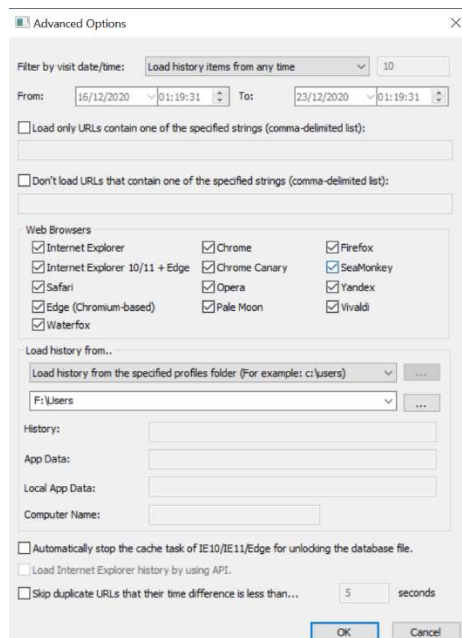


FIGURA 19 - Obter acessos a internet

https://www.skype.com/pt-br/get-skype/	Baixar o Skype Chamadas gratuitas Aplicativo de chat
https://www.skype.com/pt-br/thank-you-skype/	Obrigado por baixar o Skype
https://www.tuasaude.com/envenenamento-com-chumbinho-o-que-fazer/	Chumbinho: como o veneno age no organismo (e o que fazer) - Tua Sa...
https://www.tuasaude.com/envenenamento-com-chumbinho-o-que-fazer/	Chumbinho: como o veneno age no organismo (e o que fazer) - Tua Sa...
https://www.xvideos.com/	Vídeos pornô gratuitos - XVIDEOS.COM
https://www.xvideos.com/?k=novinha	'novinha' Pesquisar - XVIDEOS.COM

FIGURA 20 – Acesso a sites indevidos

5.9. Queira o sr perito identificar se há indícios da prática de *Fake News* no computador coletado

Resposta: Foi identificado indícios da prática de Fake News no computador coletado.

Em Windows/System32/Spool/Printers, foi identificado arquivo de impressão 00002.SPL, enviado para a pasta ANÁLISE para verificação do perito. Arquivo aberto por meio deste no software SPLView onde foi gerado um *raw file* de formato *unknown*, contendo o tamanho total de 105.420. O arquivo foi salvo no computador em .pdf, possibilitando a abertura legível do arquivo *fake news* no leitor PDF do computador do perito.

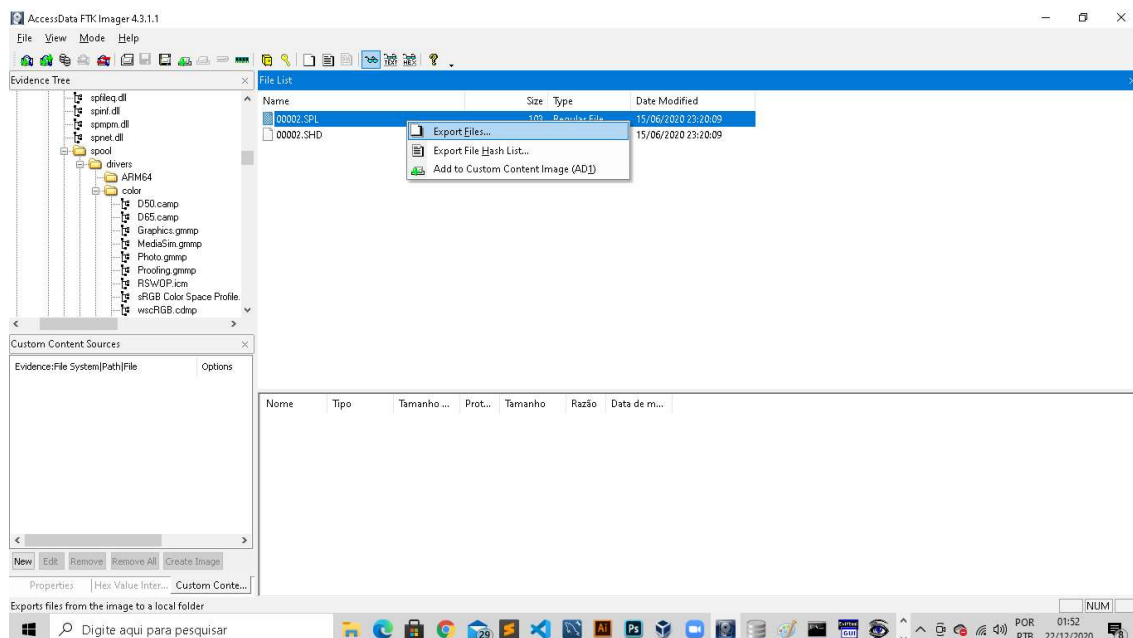


FIGURA 21 - Exportar para pasta ANÁLISE do perito

INSTITUTO DE PÓS-GRADUAÇÃO E GRADUAÇÃO MBA INFORMÁTICA FORENSE MÓDULO ASPECTOS GERAIS DA INFORMÁTICA FORENSE APLICADA

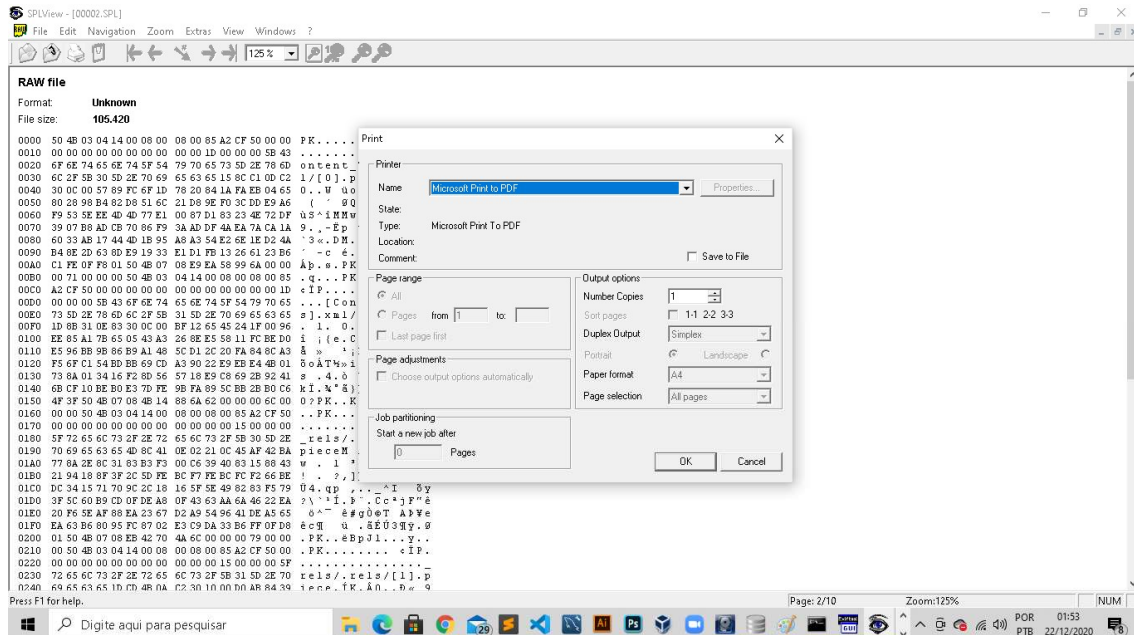


FIGURA 22 - Abrir em SplView e salvar em pdf

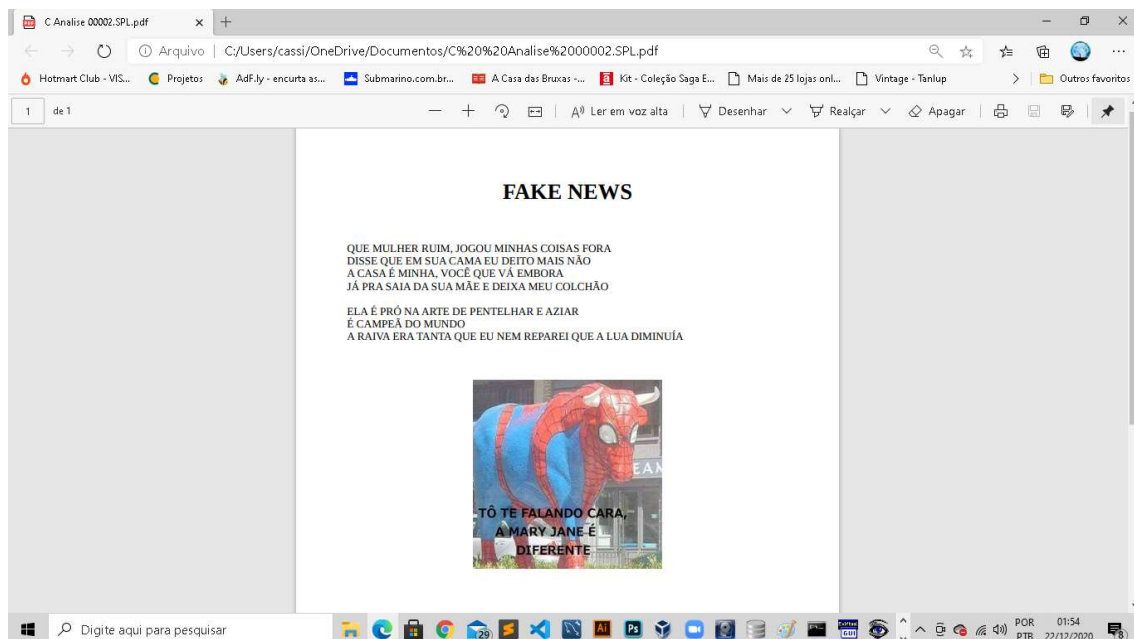


FIGURA 23 - Arquivo .pdf

5.10. Queira o sr perito identificar se há indícios de um possível planejamento para a prática de homicídio

Resposta: Foi identificado indícios de planejamento de homicídio.

MÓDULO ASPECTOS GERAIS DA INFORMÁTICA FORENSE APLICADA

Para a identificação, foi utilizada a ferramenta rip com o comando: `rip -r \Analise\NTUSER.DAT -p recentdocs ...` Verificado busca na internet de manipulação de chumbinho como consta no 33 = `search?q ...`

Também foi encontrado acessos a sites para planejamento de utilização da substância química (chumbinho) para envenenamento, com a utilização da ferramenta Browsing History View.

```

C:\WINDOWS\system32\cmd.exe
- Correlate the user SIDs to the output of the ProfileList plugin

C:\RR>rip -r \Analise\NTUSER.DAT -p recentdocs
***Hive Check***
The hive (\Analise\NTUSER.DAT) is dirty.
Please consider processing hive transaction logs via either Maxim's yarp + registryFlush.py
or via Eric Zimmerman's rla.exe.

Launching recentdocs v.20100405
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

C:\WINDOWS\system32\cmd.exe
45 = Downloads
44 = 862eba55acc6f06947592d893a2610b0.jpg
6 = PASTA_PROIBIDA
9 = Formula_Secreta.docx
32 = Applications
31 = Microsoft.Windows.Computer
43 = pthc
2 = Sistema e Segurança
1 = ::{BB06C0E4-D293-4F75-BA90-CB05B6477EEE}
38 = Preteen Nude Naked Pede best.jpg
35 = 3 boys 12yo 11yo and 7yo have fun on webcam_05.jpg
34 = Internet
33 = search?q=chumbinho+mata&elv=AXXfrEiqD9r3GuelwApulp0bAoLZL3r8d5j4o1redH1TlVSQUEf3hzmUSSTqvMdl
30 = Cotnabilidade.odt
29 = Palestra SP - Agosto2019
28 = Palestra CSI - 2 pra direito .odp
27 = MM-PLUS (D:)
23 = Disco Local (C:)
22 = HD_DO_PERITO
0 = ::{BB06C0E4-D293-4F75-BA90-CB05B6477EEE}
26 = FERRAMENTAS
25 = EVIDENCIA
8 = Este Computador
24 = C:\
20 = AULA1FCDEBI.pdf
19 = owa/
17 = lista-espera-proba-2020-1.pdf
18 = All
5 = Imagens
16 = Sem título.png
4 = Evil-Wallpapers-.jpg
13 = 192.168.10.35
  
```

FIGURA 24 - Indícios de homicídio

	https://www.tuasaude.com/envenenamento-com-chumbinho-o-que-fazer/	Chumbinho: como o veneno age no organismo (e o que fazer) - Tua Sa...	15/06/2020 18:07:50
	https://www.google.com.br/search?source=hp&ei=--LnXq21JbGz5OUPvNaLsAc&q=como+env...	como envenenar alguem com chubinho - Pesquisa Google	15/06/2020 18:07:43
	https://www.google.com.br/search?source=hp&ei=--LnXq21JbGz5OUPvNaLsAc&q=como+env...	como envenenar alguem com chubinho - Pesquisa Google	15/06/2020 18:07:59
	https://www.google.com.br/search?source=hp&ei=--LnXq21JbGz5OUPvNaLsAc&q=como+env...	como envenenar alguem com chubinho - Pesquisa Google	15/06/2020 18:07:52
	https://www.google.com.br/search?source=hp&ei=--LnXq21JbGz5OUPvNaLsAc&q=como+env...	como envenenar alguem com chubinho - Pesquisa Google	15/06/2020 18:07:43
	https://www.google.com.br/search?source=hp&ei=--LnXq21JbGz5OUPvNaLsAc&q=como+env...	como envenenar alguem com chubinho - Pesquisa Google	15/06/2020 18:08:05

FIGURA 25 – Acesso a sites de como envenenar alguém

6. CONCLUSÃO

Conforme retratado acima, foi possível verificar que:

- a) Foi identificado indícios da prática de Fake News no computador coletado, conforme figura 23 acima.
- b) Foram encontradas práticas indevidas de pedofilia, como armazenamento de arquivos e acesso a sites indevidos, conforme figuras 18 e 20 acima;
- c) Foi identificado o acesso a pasta secreta da rede com acesso e divulgação do arquivo que contém “Fórmula Secreta”, conforme figuras 13, 14, 15 e 16;
- d) Foi verificado que o suspeito acessou sites de como envenenar alguém o que evidencia um planejamento para matar uma pessoa, podendo ser um dos diretores da empresa, conforme apresentado nas figuras 24 e 25.

É o Laudo Pericial.

À consideração superior.

Goiânia, 30 de dezembro de 2020.