

FERA – Forensics Evidence Report Analyzer

Desenvolvido por: Gustavo Borelli Bedendo

26 de agosto de 2021

Sumário

1	Objetivo	2
2	I – Visualização integrada de informações	3
3	II – Mecanismo eficiente de busca	4
4	III – Módulo de observações	6
5	IV – Persistência dos registros	8
6	Outras Funcionalidades	9

1 Objetivo

Devido à crescente quantidade de dados e consequentemente do tamanho dos relatórios forenses gerados neste Instituto de Criminalística, torna-se essencial a utilização de ferramentas que facilitem a análise e visualização desses relatórios, permitindo que nós peritos, possamos organizadamente e eficientemente analisar, expor e visualizar os dados consolidados.

A ferramenta FERA (Forensics Evidence Report Analyzer), tem como objetivo organizar e auxiliar na organização dos dados na elaboração de laudos periciais e facilitar a visualização e buscas por informações nos relatórios forense, pelas partes envolvidas no processo.

Baseado nos quesitos acima, a ferramenta proposta possui quatro pilares:

- I. Visualização integrada de relatórios forenses e demais informações pertinentes.
- II. Mecanismo eficiente de busca de informações nos relatórios acima referidos.
- III. Sistema de marcação/observações de registros nos relatórios acima referidos.
- IV. Persistência dos registros criados pelos pilares I e II.

2 I – Visualização integrada de informações

Este pilar possui como preceito a simplicidade na visualização de múltiplos relatórios, permitindo maior facilidade na transição entre relatórios, aumento na organização e integração das informações e documentos pertinentes a laudo pericial. A Figura 1, apresenta a visão geral da ferramenta, em destaque o posicionamento dos relatórios forenses, laudo pericial e demais documentos pertinentes.

Todos os documentos adicionados à ferramenta são acessíveis a partir apenas de cliques no respectivo documento de interesse.

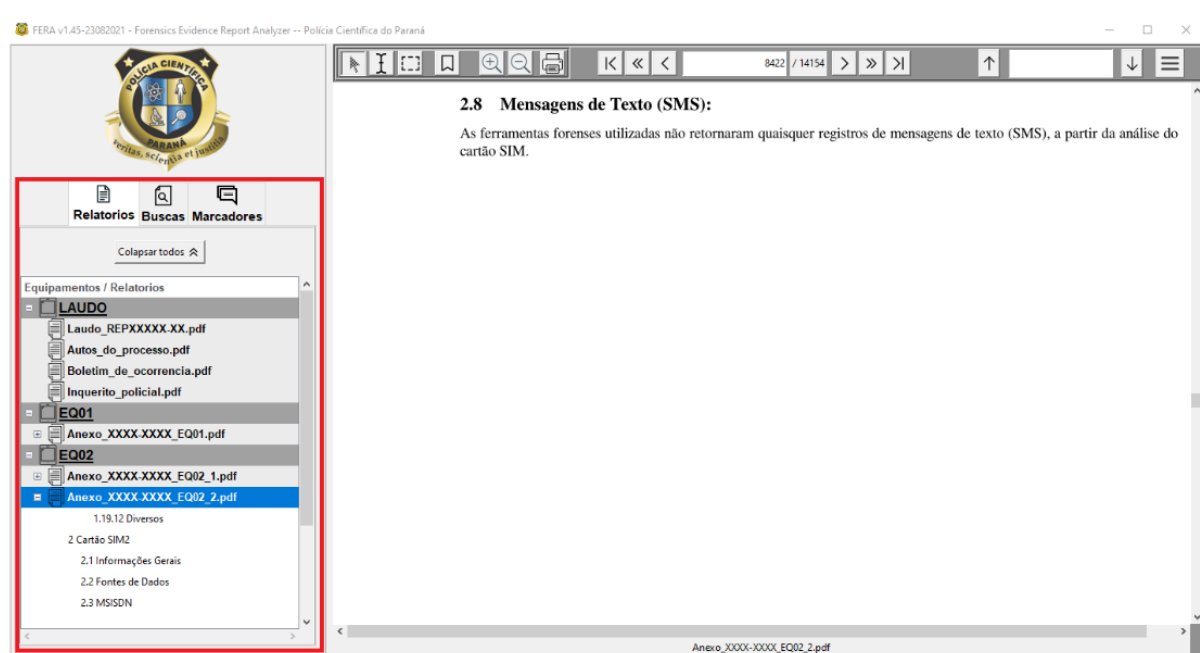


Figura 1: Visão geral da ferramenta FERA.

3 II – Mecanismo eficiente de busca

Este pilar possui como preceito a velocidade de busca por informações nos documentos adicionados à ferramenta. Por exemplo, termos e gírias relacionados ao motivo pericial, números de telefone, datas de interesse, etc. Os documentos adicionados são indexados e são passíveis de busca através de duas funcionalidades da ferramenta:

- I. Busca simples: utiliza-se do comando “LIKE” de banco de dados, assim, realiza a busca por subpalavras. Mecanismo de busca mais utilizado, pois é mais abrangente, porém é necessária filtragem dos resultados obtidos.
- II. Busca avançada: utiliza-se do comando “MATCH” de banco de dados e, especificamente, da biblioteca FTS4 (Full Text Search 4). Este mecanismo abre outras possibilidade de busca a partir de combinação de comandos pertencentes à referida biblioteca. Uma síntese desses comandos está presente na janela de busca avançada da ferramenta (Figura 3).

A Figura 2, apresenta a área de resultados de busca (3), em destaque o campo utilizado para buscas simples (1) e avançadas (2).

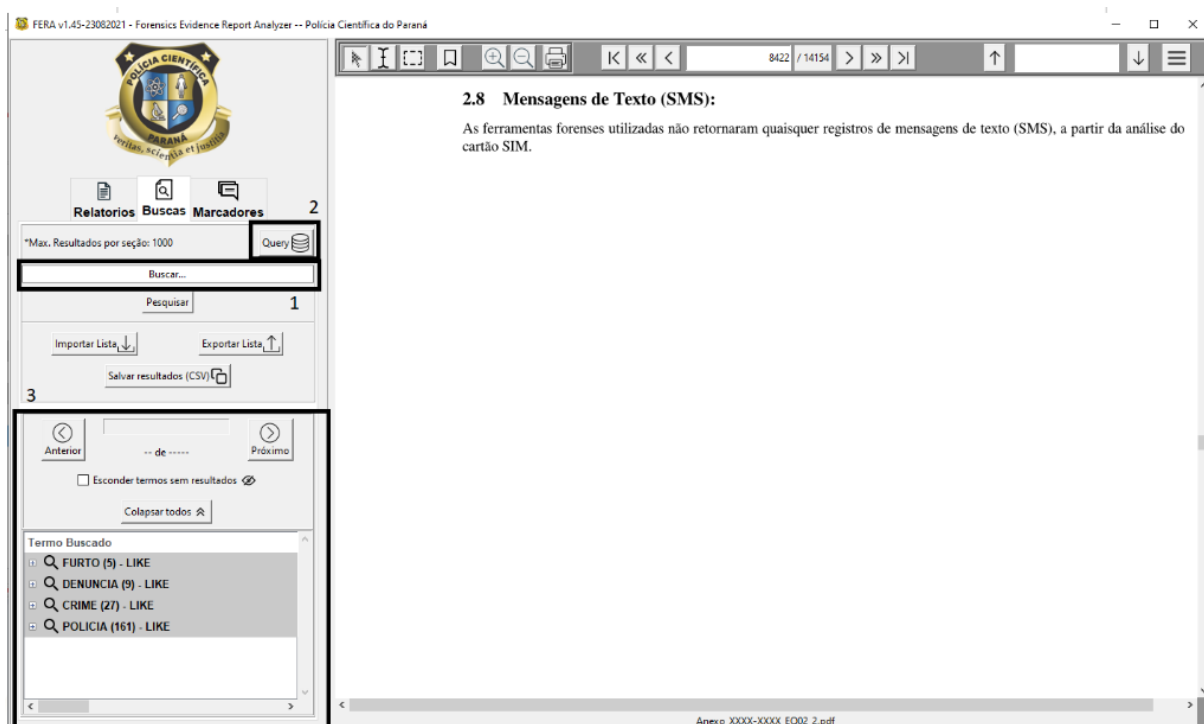


Figura 2: Visão da área de buscas e apresentação dos resultados do FERA.

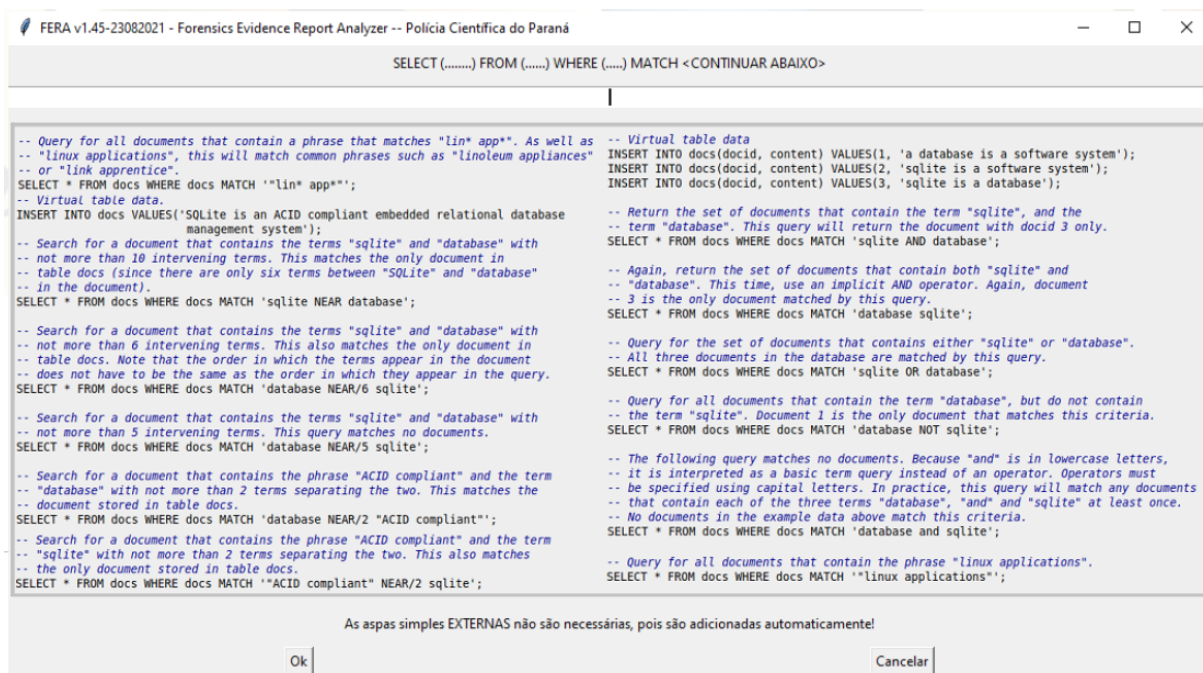


Figura 3: Lista de comandos e parâmetros da busca avançada.

4 III – Módulo de observações

Este pilar possui como preceito a organização dos registros identificados pertinentes ao motivo pericial. Através desse sistema o perito pode incrementalmente e organizadamente analisar e consolidar os registros (arquivos, conversas, eventos, etc.) nos relatórios. Ademais, permite a visualização direta desses registros pelas partes interessadas no processo. Observações podem ser adicionadas ao caso através da seleção de texto (1) ou através de uma região (2) no documento (Figura 4), com posterior clique com o botão direito (Figuras 5 e 6). As observações são vinculadas à categorias, que podem ser criadas a partir do botão “Adicionar Categoria”. Links podem ser adicionados, redirecionando a seleção (quando clicado) para outra observação, previamente adicionada. Permitindo a ligação entre observações. Tal recurso pode ser utilizado primordialmente na integração entre as referências adicionados aos laudos periciais e os relatórios forenses.



Figura 4: Modos de seleção no documento.

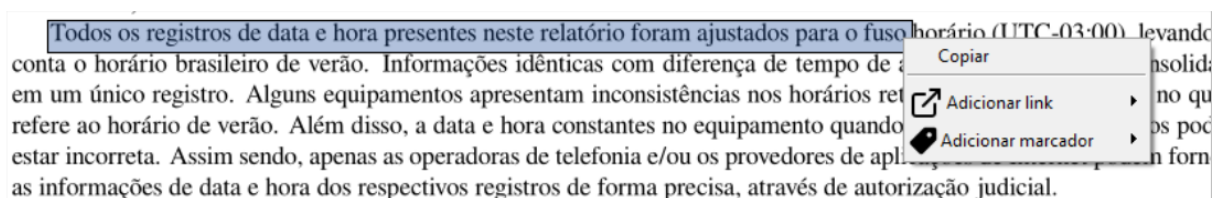


Figura 5: Modo de seleção do tipo texto.

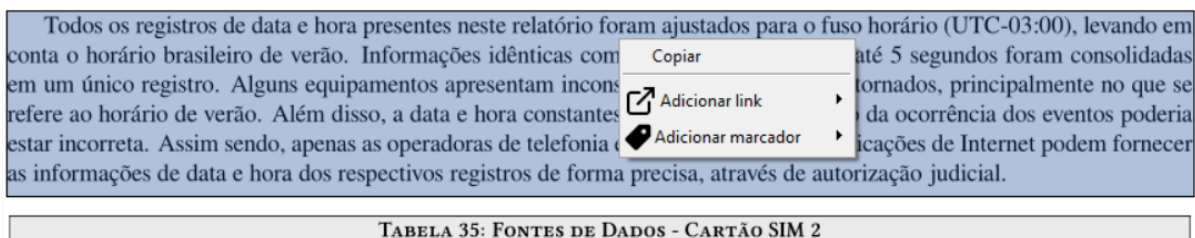
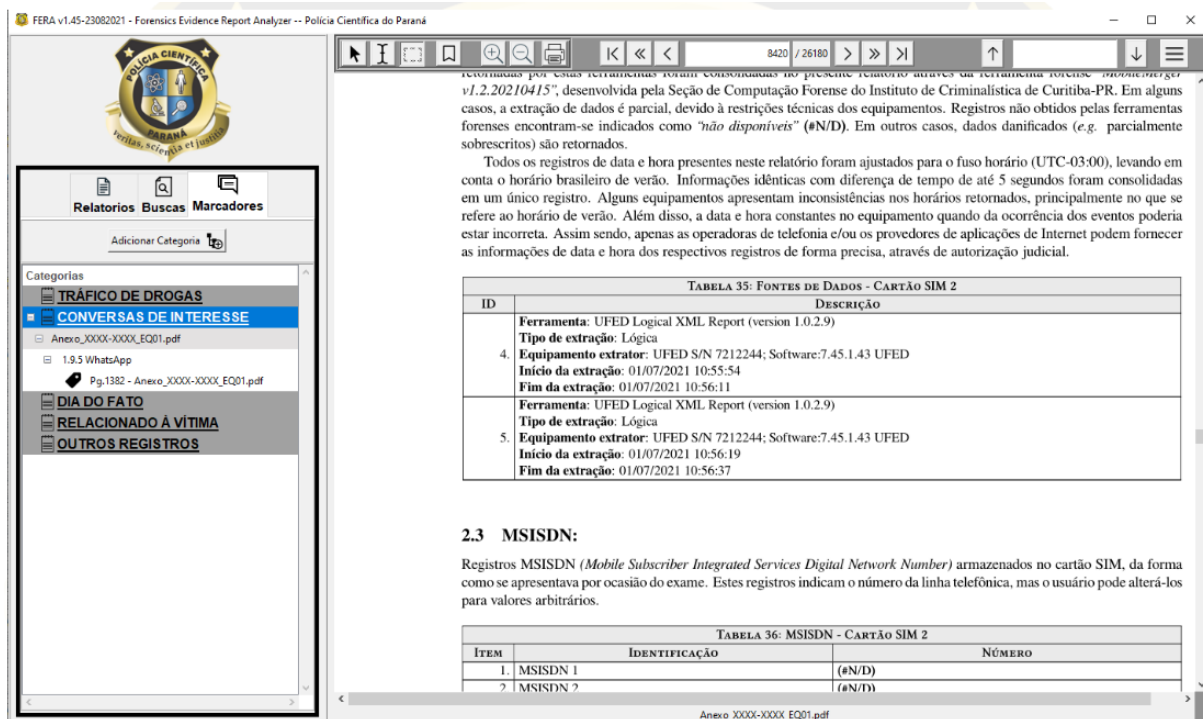


TABELA 35: FONTES DE DADOS - CARTÃO SIM 2

Figura 6: Modo de seleção por região.



FERA v1.45-23082021 - Forensics Evidence Report Analyzer -- Polícia Científica do Paraná

Relatórios Buscas Marcadores

Adicionar Categoria

Categorias

- TRÁFICO DE DROGAS
- CONVERSAS DE INTERESSE**
 - Anexo_X000X-X000_EQ01.pdf
 - 1.9.5 WhatsApp
 - Pg.1382 - Anexo_X000X-X000_EQ01.pdf
- DIA DO FATO
- RELACIONADO À VÍTIMA
- OUTROS REGISTROS

TABELA 35: FONTES DE DADOS - CARTÃO SIM 2

ID	DESCRIÇÃO
4.	Ferramenta: UFED Logical XML Report (version 1.0.2.9) Tipo de extração: Lógica Equipamento extrator: UFED S/N 7212244; Software:7.45.1.43 UFED Início da extração: 01/07/2021 10:55:54 Fim da extração: 01/07/2021 10:56:11
5.	Ferramenta: UFED Logical XML Report (version 1.0.2.9) Tipo de extração: Lógica Equipamento extrator: UFED S/N 7212244; Software:7.45.1.43 UFED Início da extração: 01/07/2021 10:56:19 Fim da extração: 01/07/2021 10:56:37

2.3 MSISDN:

Registros MSISDN (*Mobile Subscriber Integrated Services Digital Network Number*) armazenados no cartão SIM, da forma como se apresentava por ocasião do exame. Estes registros indicam o número da linha telefônica, mas o usuário pode alterá-los para valores arbitrários.

TABELA 36: MSISDN - CARTÃO SIM 2

ITEM	IDENTIFICAÇÃO	NÚMERO
1.	MSISDN 1	(#N/D)
2.	MSISDN 2	(#N/D)

Anexo_X000X-X000_EQ01.pdf

Figura 7: Visão dos marcadores (observações) criadas.

5 IV – Persistência dos registros

Este pilar possui como preceito a persistência e portabilidade dos registros adicionados à ferramenta, desta forma, os peritos podem ter continuidade na análise dos relatórios, mesmo quando interrompidos, e as partes interessadas, dada portabilidade, podem acessar os dados integralmente e na forma com o que o perito assim analisou, auxiliando a compreensão dos registros identificados por parte deste. O banco de dados e a ferramenta acompanham o Anexo Eletrônico ao laudo pericial, onde as partes envolvidas podem utilizar os mecanismos acima descritos para realizar novas análises de interesse ao processo. A ferramenta é previamente configurada pelo perito redator, bastando a execução de um dos executáveis (compatível com o Sistema Operacional presente) no diretório do Anexo Eletrônico, conforme mostrado na Figura 8.

Nome	Data de modificação	Tipo	Tamanho
Anexo	23/08/2021 15:46	Pasta de arquivos	
FERA	24/08/2021 07:48	Pasta de arquivos	
FERA-LINUX.sh	23/08/2021 11:24	Shell Script	6.710 KB
FERA-WINDOWS.exe	23/08/2021 11:29	Aplicativo	7.349 KB

Figura 8: Estrutura do Anexo Eletrônico.

6 Outras Funcionalidades

Funcionalidades complementares às anteriormente citadas, geralmente podem ser acessadas através do clique com o botão direito em observações e buscas. Conforme Figuras 9, 10 e 11. Conforme , .

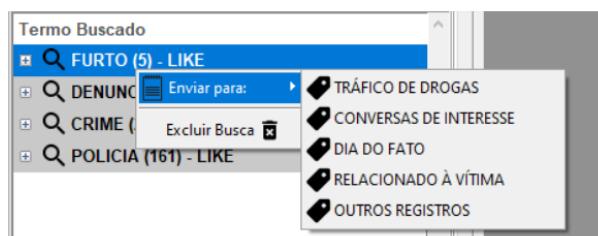


Figura 9: Exclusão e buscas e criação de observações.

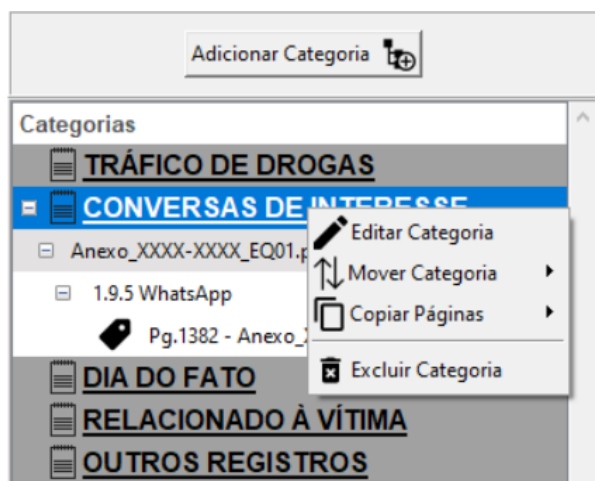


Figura 10: Gerenciamento de marcadores (categorias).



Figura 11: Busca sem persistência.

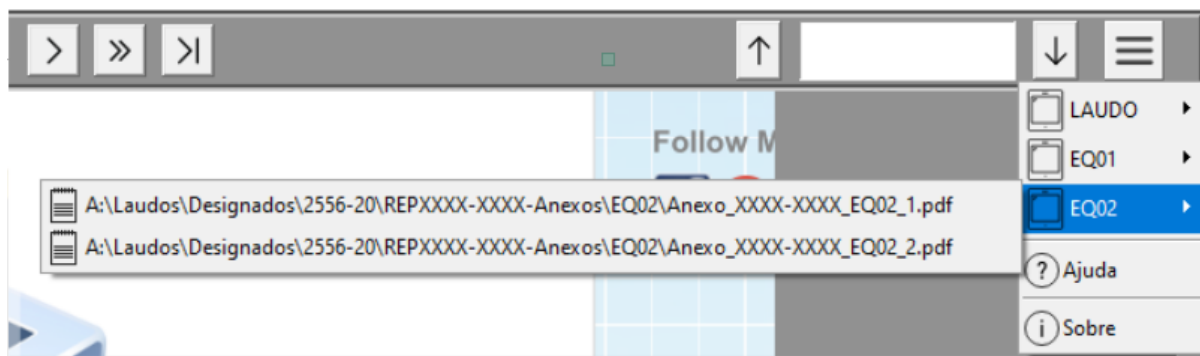


Figura 12: Botão Menu.

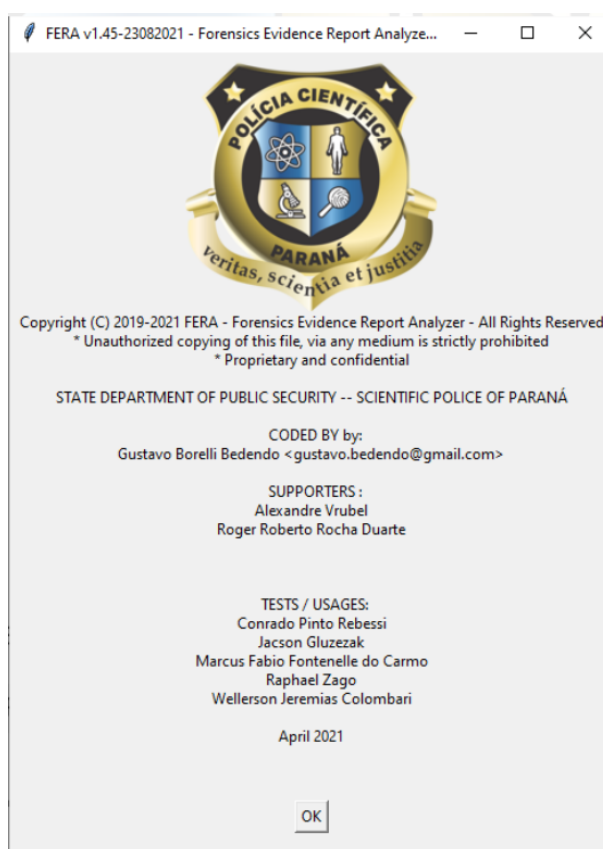


Figura 13: Créditos.