REALIZANDOEXTRAÇÃODEDADOSEMAPARELHOSANDROIDUTILIZANDOOSOFTWARE FORENSE - AVILLA FORENSICS

O *software* utilizado na extração de dados nesse tutorial é desenvolvido pelo Agente de Polícia do Estado de São Paulo, <u>Daniel Avilla</u>.

AVILLA FORENSICS é um *software* forense utilizado para realizar extrações de dados dos aparelhos móveis.



REQUISITOS MÍNIMOS:

Dispositivo: Ativado a Depuração USB. Sistema Operacional: Windows 10 atualizado. Para Extração: Sistemas 32 ou 64 Bits. Conversão Backup .AB para .TAR: Sistemas 32 ou 64 Bits e o JAVA instalado. Relatório IPED PF: Sistema 64 Bits e JAVA 64 Bits instalado.

PROGRAMAS NECESSÁRIOS:

DOWNLOAD AVILLA FORENSICS: DOWNLOAD AQUI

DOWNLOAD JAVA: DOWNLOAD AQUI

DOWNLOAD WINRAR: DOWNLOAD AQUI

VÍDEO TUTORIAL:

https://youtu.be/KuSmct1Qa30

PREPARANDO O APARELHO CELULAR

Para iniciarmos devemos preparar o aparelho celular para que seja feita a comunicação com o *ADB* - *Android Debug Bridge*, para isso iremos ativar o **MODO DEPURAÇÃO USB** do aparelho celular, princípio básico utilizado nas extrações forense em dispositivos móveis (android).

SIGA FIELMENTE AS ETAPAS:

Acesse as **configurações do aparelho celular** e desce até a opção **Sobre o telefone**.



Entre na opção **Informações do software**, e vá até a opção **Número de compilação** e clique 7 (sete) VEZES.



Durante esse processo o aparelho irá exibir um alerta informando quantas etapas faltam para liberar o **MODO DESENVOLVEDOR**.

Faltam 4 etapas para você se tornar um desenvolvedor.

Quando liberado o sistema irá exibir o seguinte alerta:



Após liberado o **MODO DESENVOLVEDOR**, volte em "**Configurações**" e role a barra lateral até o final. Você vai perceber que o "**Modo Desenvolvedor**" foi ativado e já aparece nas opções.

ி 🗖 🛄 ளி 30% 🖬 19:36	🗟 🖬 📶 🗐 30% 🖬 19:		
esquisar ෫ 🛞 < OPÇÕES DO DESENVOLVEDOR		t (
	ΑΤΙΛΑΡΟ		
loqueio e Segurança Visplay, Reconhecimento facial,	Fazer relatório de erro		
contas oud, Fazer backup e restaurar,	Senha de cópia de segurança da á	rea d	
es do Google	Os backups completos da área de trabalho não são protegidos.		
	Permanecer ativo		
idade ão, Habilidade manual e intera	A tela nunca ficará suspensa durante o carregamento	0	
mento geral Irada, Data e hora, Restaurar	Registro de investigação HCI BI Capturar todos os pacotes Bluetooth HCI em um arquivo.	0	
ão de software	Convisoo om funcionomonto		
zações, Atualiz, de software ag	Ver e controlar os servicos sendo executados		
o usuário	atualmente.		
elefone mações legais. Nome do dispo	Modo de cor da imagem Usar sRGB	0	
lo desenvolvedor	Implementação do WebView Chrome		
	Ioqueio e Segurança iisplay, Reconhecimento facial, contas oud, Fazer backup e restaurar, es do Google idade ao, Habilidade manual e intera mento geral rrada, Data e hora, Restaurar ão de software zações, Atualiz. de software ag o usuário suário elefone mações legais, Nome do dispo	Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) 1930 Image: Analoge (a) in solve (a) in solve (a) in analoge	

ATENÇÃO NESSA ETAPA!

Dentro das **OPÇÕES DO DESENVOLVEDOR**, iremos ativar o modo **DEPURAÇÃO USB**.



PERMITIR A DEPURAÇÃO USB?

Clique em OK.

Ainda dentro das Opções do Desenvolvedor **ATIVE** também a opção **PERMANECER ATIVO**.



Feito esses passos conecte o aparelho celular na porta USB do computador e permita o acesso ao telefone assim que for solicitado.



*** Quando o aparelho celular é conectado na porta USB do computador a seguinte caixa de alerta é informada pelo Windows. Esse alerta informa que o aparelho celular está em comunicação com o sistema operacional.



Esses são os passos necessários para deixar o aparelho celular preparado para ser utilizado no Avilla Forensics.

*** As opções Sobre o telefone, Informações do software e Número de compilação, podem variar o local de onde são encontradas, dependendo do fabricante do aparelho, modelo e versão do android. Basta uma busca no Google "como liberar o modo desenvolvedor do aparelho XYZ", para encontrar informações precisas de um determinado modelo/fabricante.

INFORMAÇÃO IMPORTANTE

Após realizar o download do AVILLA FORENSICS (<u>download aqui</u>), o software vem zipado (.zip), use o WINRAR (<u>download aqui</u>), e descompacta o arquivo dentro do MEU COMPUTADOR => DISCO LOCAL (C:)

Disco Loc	:al (C:)			
13,0 GB li	vre(s) de 222 GB			
	6 720			
Este Computador 🔸 Disco Loca	al (C:) >			
	Nome	Data de modificação	Тіро	Tamanho
# # # # #	SWinREAgent android Arquivos de Programas Arquivos de Programas (x86) Arquivos de Programas RFB forensics ARQUIVO DESCOME MSOCache PerfLogs ProgramData Usuários Windows	12/03/2022 20:32 11/03/2022 21:40 11/03/2022 21:39 11/03/2022 21:39 26/02/2021 19:44 09/03/2022 19:54 *ACTADO 19/02/2022 13:32 03/12/2019 12:08 07/12/2019 06:14 13/03/2022 12:53 17/01/2022 19:26 10/04/2021 19:23 13/03/2022 02:08 26/12/2019 09:20	Pasta de arquivos Pasta de arquivos	1 КВ
	🖉 forensics 🛹 🕇	Abrir Abrir Abrir com o WinRAR Extrair arquivos Extrair aqui Extrair aqui Compartilhar	Arquivo ZIR do Wi.	1 KB 926.868 KB
stema (D:)		Abrir com Verificar com o Malwarebyte Renomear Avançado Restaurar versões anteriores	5	
) stema (l:) Y:)		Enviar para Recortar	<u>></u>	
		Copiar Criar atalho Excluir Renomear Propriedades		

REALIZANDO EXTRAÇÃO LÓGICA – BACKUP ADB - ANDROID

Dentro da pasta **forensics**, clique com o **botão direito** em cima do arquivo **Avilla_Forensics** e clique para executá-lo como administrador.



Com o Avilla Forensics aberto iremos começar a realizar a extração LÓGICA do aparelho celular. O primeiro passo é realizar o teste de conexão entre o celular e o software.

- 1) Entre na opção BACKUP ADB.
- 2) Clique em TESTAR CONEXÃO.

Avilla Forensi	rsics 3.0 - [Extração Lógica Android]	- 0 X
E	1	. 5)
Coletas Android	ad 😫 🕒 🔯 🛄 🚺 의 🏟 Coletas IOS 🏟	
Ferramentas 🗂		
	Extração Lógica Android	Testar Conexão: Salvar em: Extrair
ω	Destino:	2 Ative o modo DEPURAÇÃO USB
.tar		
~	W	
Contraction of the second seco		·
APK		
V		

Se estiver ocorrendo comunicação entre o aparelho celular e o software, irá aparecer na "List of devices attached", o modelo do aparelho celular.

List of devices attached R9XN402XLJB device product:a01qub model:SM_A015M device:a01q transport_id:1

O próximo passo é escolher a pasta onde será salvo a extração, basta clicar em "SALVAR EM:" e selecionar a pasta.

>> Destino: C:\Users\PCMG-AIP\Desktop\TUTORIAL\EXTRACAO\backup-2022-03-14-09-22-33.ab

Feito isso clica em "EXTRAIR".

Quando iniciar o processo de extração irá aparecer caixas de alertas, leia com atenção e siga fielmente as instruções.

Atenção	×
Este processo pode demorar minutos preste atenção no backup completo dispositivo, coloque uma senha caso	s ou até horas, durante a coleta que sera solicitado na tela do o necessário.
	ОК

Nesse momento no aparelho celular irá aparecer a tela de **BACKUP**, se estiver habilitada a opção **FAZER BACKUP DE MEUS DADOS** basta clicar nela, se

não, informe uma senha de sua escolha para que a opção fique habilitada. Pode utilizar uma senha básica padrão, como exemplo 12345.



O software começará a fazer o backup dos dados do aparelho celular, basta aguardar a conclusão do processo.

Quando a extração for concluída será informado na tela de informações do software, conforme imagem a seguir:

List of devices atta	ched
R9XN402XLJB	device product:a01qub model:SM_A015M device:a01q transport_id:1
>> Destino: C:\Us	ers\PCMG-AIP\Desktop\TUTORIAL\EXTRACAO\backup-2022-03-14-09-31-03.ab
>> Extração Inicia	a. (14-03-2022-09-31-22)
>> Gerando logs,	guarde (14-03-2022-09-41-24)
>> Tamanho do ar	guivo .ab: 2436222277 bytes
>> Hash MD5 do a	rguivo .ab: c23f92bb7d13d5db48b38960eed8115c
>> Hash SHA-256	do arguivo .ab; cf2fc68b0f51427621a0df35c9b0fba5b5436d6543f291064ab02a3c03d5c22b
>> Logs Gerado (4-03-2022-09-41-47)
>> Extração Cono	

A extração no formato **.AB** estará na pasta que foi selecionada no início do processo, que no caso do tutorial é **DESKTOP\TUTORIAL\EXTRACAO**.

Assim fica concluído o módulo de extração lógica **BACKUP ADB** do **Avilla Forensics**.

Mais adiante iremos fazer a conversão do arquivo **.AB** para **.TAR**, extensão de arquivo que é aceito pelo software **IPED** da **Polícia Federal**.

APK DOWNGRADE - EXTRAÇÃO DE DADOS WHATSAPP – ANDROID

Agora que você já esta mais familiarizado com o Avilla Forensics, acesse a opção APK DOWNGRADE.



Clique em **TESTAR CONEXÃO**, e se a comunicação estiver OK, irá apresentar a "**List of devices attached**" o **modelo do aparelho celular**, da mesma forma que realizamos no passo anterior do tutorial.

O próximo passo é clicar em APLICAÇÃO TESTE, nesse momento será instalado no aparelho celular o aplicativo "Aplicacao Teste".



Perceba-se que o aplicativo teste vai estar aberto na tela do aparelho celular.

Realizado essas etapas o próximo passo é escolher qual aplicativo iremos realizar o downgrade, que no nosso caso do tutorial será o Whatsapp. Para isso clique em DETECTAR.



Selecione o com.whatsapp.

Agora basta clicar em **SALVAR EM:** e selecionar a pasta que a extração será salva.

ATENÇÃO!

Nas próximas etapas, siga fielmente as instruções que serão apresentadas nos alertas do **Avilla Forensics** e também na **tela do aparelho celular**.

Clique em **EXTRAIR**.



Pasta Backup do base	.apk:
Nome	Data de modificação
<i>⊘base</i>	14/03/2022 10:57

PASTA BACKUP localizado no canto inferior direito do Avilla Forensics.



O alerta informa que será necessário reiniciar o aparelho celular, clique em sim.



Clique em OK somente após o aparelho celular ter reiniciado por completo e caso tenha senha e/ou bloqueio de tela, certifique-se que tenha feito o desbloqueio do mesmo.

ATENÇÃO NESSA ETAPA!



Nesse momento foi desinstalado a versão atual do **Whatsapp** e instalado uma versão exploit do aplicativo (**com.whatsapp**), para dar as permissões necessárias, abre o aplicativo no aparelho celular e clique em **CONTINUAR**.



Após clicar em **CONTINUAR**, volte para o **Avilla Forensics** e clique em OK.

14:09 🛈		14:09 🖸	⊖ ▼ 4ª ⊿ 😡
Backup completo		Backup completo	
Foi solicitado um backup completo de para um computador conectado. Quer aconteça?	todos os dados permitir que isso	Foi solicitado um backup co para um computador conec aconteça?	ompleto de todos os dados ctado. Quer permitir que isso
Caso você não tenha solicitado o back a operação prossiga.	up, não permita que	Caso você não tenha solicit a operação prossiga.	tado o backup, não permita que
Se você deseja codificar os dados de b insira uma senha abaixo:	aackup por completo,	Se você deseja codificar os insira uma senha abaixo:	dados de backup por completo,
	<u>``</u>	com.whatsapp	
Não fazer backup Faz	ter backup de meus dados	Não fazer el car	do backup dados

Nesse momento no aparelho celular irá aparecer a tela de **BACKUP**, se estiver habilitada a opção **FAZER BACKUP DE MEUS DADOS** basta clicar nela, se não, informe uma senha de sua escolha para que a opção fique habilitada. Pode utilizar uma senha básica padrão, como exemplo 12345.



Clique em Sim.

>> Tamanho do arquivo .ab: 40201221 bytes
 >> Hash MD5 do arquivo .ab: 204aa7a841541b69434c4eaa8f4a6526
 >> Hash SHA-256 do arquivo .ab: 3cb996f3d4207ee8c4d688368167021ed208f9f520b14016c0d0770b6e67a23e
 >> Logs Gerado (14-03-2022-11-27-22)
 >> Extração do com.whatsapp concluída (14-03-2022-11-27-22)

Extração concluída.

CONVERTER .AB PARA .TAR E UTILIZAR O SOFTWARE IPED DA POLÍCIA FEDERAL PARA INDEXAR OS ARQUIVOS EXTRAÍDOS

Realizada as extrações **BACKUP ADB** e **APK DOWNGRADE**, agora iremos fazer a conversão dos arquivos .**AB** para **.TAR** para que seja possível realizar a analise do conteúdo que foi extraído do aparelho celular.



Entre na opção destacada para realizar a conversão.

Em SELECIONAR, escolha o arquivo .AB que foi realizado na extração BACKUP ADB, em seguida escolha o local onde será salvo o arquivo na extensão .TAR.

*** Eu salvo dentro da mesma pasta que foi criada quando foi realizada a extração, para que fique juntos tanto o arquivo .AB quanto o .TAR.

Converter Backu	o .AB para .TAR:		
	C:\Users\PCMG-AIP\Desktop)\backup-2022-03-14-09-31-03.ab
	C:\Users\PCMG-AIP\Desktop		Nbackup tar-2022-03-14-13-32-23.tar
.tar	O Backup sem senha (Backup com senha ATENÇÃO!!!	Requisito: Instalar Java https://www.java.com/pt-BR/download/
>> Origem: C:\Us >> Destino: C:\U	sers\PCMG-AIP\Desktop\ sers\PCMG-AIP\Desktop\	TUTORIAL\EXTRA \TUTORIAL\EXTR	ACAO\backup-2022-03-14-09-31-03.ab ACAO\backup-tar-2022-03-14-13-32-23.tar

Repare que o destino da pasta no .TAR é o mesmo do .AB.

Se no momento de realizar a extração você informou uma senha para ativar a opção FAZER BACKUP DE MEUS DADOS, nesse momento você deve marcar BACKUP COM SENHA e quando clicar em CONVERTER, será solicitado a senha e você deve digitá-la no campo informado.

Digite a senha definida no Backup:
Destino:
12345

Agora aperte OK e a conversão irá se iniciar.

>> Origem: C:\Users\PCMG-AIP\Desktop\TUTORIAL\EXTRACAO\backup-2022-03-14-09-31-03.ab >> Destino: C:\Users\PCMG-AIP\Desktop\TUTORIAL\EXTRACAO\backup-tar-2022-03-14-13-32-23.tar >> Conversão .AB para .Tar iniciada. <</td>

>> Conversão Concluida.

Conversão concluída. Agora o arquivo no formato **.TAR** estará dentro da pasta selecionada.



Faça o mesmo processo para a extração APK DOWNGRADE (whatsapp).



*** Como realizamos dois tipos de extração o **BACKUP ADB** e **APK DOWNGRADE**, vamos criar uma nova pasta e incluir todos os arquivos necessários para realizarmos a indexação do **IPED**.

me	Data de modificação	Тіро	Tamanho
COLETA -	14/03/2022 12:01	Pasta de arquivos	
EXTRACAO	14/03/2022 09:41	Pasta de arquivos	
WHATSAPP	14/03/2022 11:27	Pasta de arquivos	

Criei uma nova pasta com o nome **COLETA**.

Repare na imagem que possuí três pastas, sendo elas:

EXTRACAO: pasta contendo a extração BACKUP ADB.

WHATSAPP: pasta contendo a extração APK DOWNGRADE (Whatsapp). COLETA: pasta que iremos juntar os arquivos convertidos em .TAR das extrações BACKUP ADB e APK DOWNGRADE juntamente com a pasta com.whatsapp ou Whatsapp.

*** Quando a biometria do aparelho celular estiver desativada, por padrão os arquivos de mídias são salvos no seguinte caminho:

/sdcard/WhatsApp

Agora quando o usuário ativa a biometria as mídias passam a serem salvas no caminho abaixo:

/sdcard/Android/media/com.whatsapp/

Por isso é preciso ficar atento a esse detalhe para saber qual a pasta deve ser selecionada no momento que for fazer a indexação.

No aparelho celular utilizado na produção desse tutorial, a biometria estava ativada.

Então, dentro da pasta **COLETA** incluímos os arquivos de extração:

- 1) backup-tar-2022-03-14-13-32-23 (BACKUP ADB);
- 2) backup-tar-2022-03-14-13-43-50 (APK DOWNGRADE);
- 3) e a pasta com.whatsapp (pasta que contém os arquivos de mídia).

Ficando da seguinte forma:

RIAL > COLET	Α >	
Nome	^	Data de modificação
com.whats	app	14/03/2022 12:00
🙀 backup-tar	-2022-03-14-13-32-23	14/03/2022 13:40
🙀 backup-tar	-2022-03-14-13- <mark>4</mark> 3-50	14/03/2022 13:43

Nome	Data de modificação	Tipo
Shared	14/03/2022 12:00	Pasta de arquivos
.StickerThumbs	14/03/2022 11:24	Pasta de arquivos
.Thumbs	14/03/2022 11:24	Pasta de arquivos
trash	14/03/2022 11:24	Pasta de arquivo:
Backups	14/03/2022 12:00	Pasta de arquivos
Databases	14/03/2022 12:00	Pasta de arquivo
Media	14/03/2022 12:00	Pasta de arquivo

Organizado a nossa estrutura de pasta, agora iremos realizar a indexação da pasta para que seja possível realizar a analise do conteúdo através do IPED.



Acesse a opção do IPED.

Marque a opção INDEXAR PASTA.



Em **SELECIONAR** informe o caminho da pasta que criamos no caso do tutorial a pasta **COLETA**.



Em SALVAR EM: seleciona a pasta que ficará salva a indexação do IPED.

Para ficar organizado, cria uma nova pasta e nomeia-a por IPED.





Assim ficou a estrutura do processo.

Agora clique em **GERAR**.

🛓 Indexador e Processado	or de Evidência	as Digitais 3.18.12			-	
	Processing 2144 / 13479 - Finish in 0h 2m 44s					Pause
Statistics:	a	Task Times:		Parser Times:		Current Iten
Processing Time	0h 0m 46s	SkipCommitedTask	0s (0%)	CompressorParser	0s (0%)	Worker-0
Estimated Finish	0h 2m 44s	IgnoreHardLinkTask	0s (0%)	EmptyParser	0s (0%)	Worker-1
Average Speed	70 GB/h	TempFileTask	-	EmptyVideoParser	0s (0%)	Worker-2
Current Speed	88 GB/h	SignatureTask	1s (3%)	HtmlParser	0s (0%)	Worker-3
Volume Found	4,191 MB	SetTypeTask	0s (0%)	ImageOCRMetadataParser	0s (0%)	Worker-4
Volume Processed	1,011 MB	SetCategoryTask	0s (0%)	OOXMLParser	0s (0%)	Worker-5
Items Found	13479	RefineCategoryTask	0s (0%)	OggParser	0s (0%)	Worker-6
Items Processed	2145	HashTask	1s (3%)	PDFOCRTextParser	0s (0%)	Worker-7
Actual items processed	1418	KFFTask	-	PackageParser	0s (0%)	Worker-8
Subitems Processed	747	LedKFFTask	-	RawStringParser	0s (0%)	Worker-9
Carved items	0	ProjectVICHashLookup	-	TXTParser	0s (0%)	Worker-10
Carved discarded	0	DuplicateTask	0s (0%)	WebPParser	0s (0%)	Worker-11
Exported items	727	AudioTranscriptTask	-	WhatsAppParser	0s (0%)	
lanored items	0	VideoThumbTask	9s (31%)	XMLParser	0s (0%)	

O indexador IPED irá começar a carregar as informações.

>> 0	Drigem: C:\Users\PCMG-AIP\Desktop\TUTORIAL\COLETA
>> D	Destino: C:\Users\PCMG-AIP\Desktop\TUTORIAL\IPED
>> In	ndexação IPED iniciada. 🔫 🗕 🚽
>> In	ndexador Gerado. 🚄

Indexador gerado.

Agora dentro da pasta **IPED** terá o arquivo do indexador **IPED-SearchAPP**, basta dar dois cliques e o mesmo irá abrir com o resultado da extração.



O IPED é um poderoso software desenvolvido por Peritos Criminais da Polícia Federal capaz de lidar com alto processamento de dados, vale destacar que tal ferramenta foi amplamente utilizada na operação Lava Jato.

https://servicos.dpf.gov.br/ferramentas/IPED/

https://github.com/sepinf-inc/IPED

TELAS DO IPED



Hex Text Metadata d Preview	Hex Text Metadata I Preview			
WhatsApp Chat - Cristina -	WhatsApp Chat - Panorama -			
2020-09-22	NO CONTRACTOR			
Messages to this chat and calls are now secured with end-to-end encryption. Tap for more	2020-07-17 14:27:08 -03:00			
mio. 2020-05-22 15-33-11-05-00	2020-07-17 14:27:59 -03:00 🖋			
Cristina @s.whatsapp.net) Esperar ela ficar um pouco melhor ela vai decidir amanhã te dou a resposta obrigada! 2020-09-22 19:51:30-03:00	IMAGENS =>			
2020-09-23	Audio Message File			
Cristina (3. s. whatsapp.net) Message deleted from sender. 2020-09-23 06:19:00 -03:00	9.5.0.4 S. 3.6 V			
Cristina (2020-09-03-00) Message deleted from serider. 2020-09-23 06:20:39-03:00	2020-07-17 14-28-27-03-00			
Cristina Construction (Construction) Cristina (Constru	Panorama (35 whatsapp.net) Blz obrigado 2020-07-17 14:34:12 -03:00			
	2020-08-04			
2020-09-23 06:22:58-03:00 Cristina Audio Message File	IMAGENS => 2020-08-04 08:26:29 -03:00 *			