CLAUDIO JOEL BRITO LÓSSIO

Manual descomplicado de *COMPLIANCE* TÉCNICO-LEGAL em **CLOUD FORENSICS**

Guia para Profissionais do Direito
e da Informática Forense

2022

EDITORA
*Jus*PODIVM
www.editorajuspodivm.com.br

5

CONFORMIDADE TÉCNICA

A conformidade técnica relaciona-se com a aplicação das diretrizes formuladas pelas normas ISO, de acordo com as necessidades de utilização e com o recurso a ferramentas lógicas, e *softwares* adequados para que a recolha de evidências e o procedimento de aquisição até à preservação tenham o máximo de conformidade, desse modo minimizando possíveis objeções. Neste capítulo, serão apresentados alguns procedimentos iniciais para que seja assegurada a conformidade técnica, bem como garantido o rito de aquisição.

O *Compliance* é sinônimo de conformidade preventiva e, como é um termo que vem ganhando proeminência global quando se aborda a questão da prevenção, é comum que ele seja convocado para textos científicos, como é o caso.

Assim, iniciamos a apresentação dessa resposta a incidentes de segurança da informação abordando a sua conformidade técnica, quando se trata de *Cloud Forensics*.

O consumidor é a pessoa que utiliza os serviços de um fornecedor de conteúdo ou de outros, como um fornecedor de serviços de armazenamento em *cloud*. O procedimento de aquisição do conteúdo pode ser realizado por diversos métodos distintos, alguns com base no consumidor e outros no fornecedor. (Manral, Bharat, *et al*., 2019)

A aquisição realizada pelo consumidor fica completamente limitada, visto que o procedimento e o acesso físico estão, muitas vezes, indisponíveis. Assim, o consumidor poderá solicitar que o procedimento de aquisição seja concretizado pelo fornecedor, mas existem dois fatores fulcrais que devem ser tidos em conta: o tempo e o espaço. E importa recordar que, por vezes, esse procedimento está indisponível. (Manral, Bharat, *et al*., 2019)

O procedimento de aquisição numa possível resposta a um incidente de segurança informática pode ser visualizado de duas formas, uma a ocorrer com monitorização prévia, a segunda apenas após o evento; trata-se, por isso, de medidas e métodos prévios ou posteriores ao evento. Por exemplo, recolher previamente *logs* poderá constituir uma base comparativa para *logs* futuros, possibilitando assim uma maior hipóteses de sucesso (Manral, Bharat, *et al*., 2019). Neste texto, focamos nos métodos realizados posteriormente ao incidente de segurança informática, ainda que nada impeça a análise dos *logs*.

O tempo deve ser o menor possível, e as políticas internas do fornecedor nem sempre contemplam a logística necessária para tal procedimento de aquisição. Já o espaço fica limitado ao território, ou, caso seja necessário esperar pela cooperação internacional, ligado à problemática do

fator tempo. Ainda assim, ao contratar uma *Cloud* que possibilite uma maior autonomia do consumidor, como a IaaS, o contratante poderá utilizar mecanismos para monitorização de eventos, por exemplo.

Existem alguns procedimentos basilares que devem ser seguidos perante um mandado judicial para uma aquisição envolvendo a *Cloud* de uma forma mais eficiente, conforme a imagem abaixo:

Figura 9 – Forense em Cloud por mandado judicial

- Assegurar a posse de um mandado judicial, pois, sem ele, o acesso a uma conta em *cloud* por parte do perito constituirá um acesso ilegítimo; tal situação, além de poder tipificar um crime e invalidar todo o processo, tornará nulas quaisquer provas e outros procedimentos delas derivados;
- Obter credenciais de acesso é essencial para que seja acedido qualquer dado que esteja em *cloud*, tanto para procedimentos manuais como através da utilização de ferramentas forenses;
- Impossibilitar o acesso às credenciais por terceiros. Pode-se fazê-lo alterando a senha de acesso e removendo o *e-mail* e telefone para recuperação, ou qualquer outro mecanismo de segurança que possibilite a quebra do acesso. Este procedimento é o que bloqueia o acesso à conta daquelas credenciais, preservando desse modo a sua disponibilidade para os peritos;

- Depois de assegurado o acesso à conta, iniciar o processo de aquisição, que pode ser realizado utilizando ferramentas profissionais ou no modo manual.

No âmbito privado, em procedimentos internos das pessoas coletivas, a aquisição forense em *Cloud* numa possível resposta a incidentes deve igualmente seguir um procedimento baseado nos padrões técnicos internacionais e nas políticas internas corporativas.

Importa compreender o que é o procedimento para investigações internas. Num tal cenário, pode observar-se o seguinte:

Figura 10 – Forense em Cloud por determinação da Organização

Devemos estar plenamente cientes de que a realização de um processo forense em *cloud*, numa possível resposta a um incidente, deve respeitar a sequência de procedimentos determinados pelas normas técnicas de padrão internacional, ISO 27035 e ISO 27037, tal como descrita na figura a seguir. (Garrison, 2010)

Figura 11 – Processo Forense

Qualquer procedimento de aquisição, com recurso a ferramentas ou não, necessita de credenciais de acesso às

contas em *cloud*, de modo a possibilitar o procedimento de forense digital na investigação de dispositivos locais como computadores, *smartphones*, IoT, entre outros dispositivos. Nesse contexto, a obtenção das credenciais é necessária para se conseguir o acesso de fornecedores de conteúdo em *cloud*. Assim, apresentamos abaixo algumas ferramentas:

O *WebBrowserPassView* é uma ferramenta gratuita da Nirsoft, que possibilita a visualização das credenciais armazenadas nos *browsers* de um computador. É bastante utilizado para, pelo menos, realizar um primeiro acesso ou criação de conta.

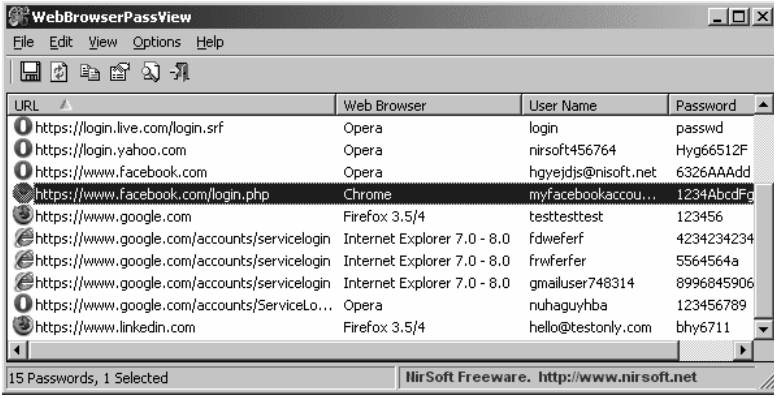

Figura 12 – WebBrowserPassView

Fonte da Imagem: https://www.nirsoft.net/utils/web_browser_password.html.

O *Remote Desktop PassView* é uma ferramenta equivalente à anterior, embora seja vocacionada para o acesso às credenciais armazenadas no *Remote Desktop Connection*.

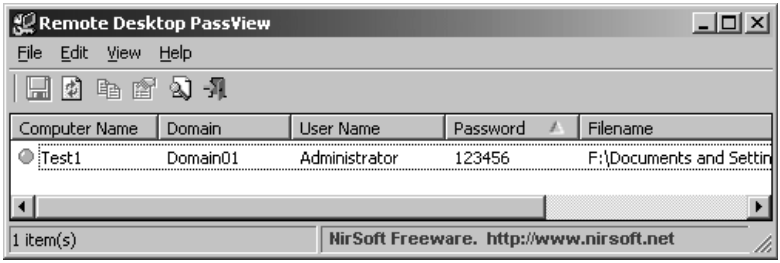

Figura 13 – Remote Desktop PassView

Fonte da Imagem: https://www.nirsoft.net/utils/remote_desktop_password.html.

O *Autopsy* é uma ferramenta que está presente em muitos dos procedimentos que envolvem o forense digital; pode ser utilizado para realizar o exame e facilitar a análise de evidências recolhidas localmente, por *snapshot* ou através da cópia de dados dos fornecedores de serviço.

Para essa ferramenta existem ainda os Ingest Modules, suplementos que podem ser agregados ao Autopsy e assim oferecer mais recursos. Referenciamos aqui o *Chrome Passwords* e o *Google Drive Analyzer* (Autopsy, 2020), que podem ser utilizados de forma gratuita.

A ferramenta *XRY* da MSAB promete recolher os *tokens* das credenciais de aplicativos e serviços *Cloud* presentes num dispositivo móvel, ou simplesmente efetuar a aquisição do conteúdo nesses fornecedores de conteúdos em *Cloud*. Esta ferramenta é paga.

Importa recordar que, quando acima nos referimos à descoberta de credenciais, falamos, por exemplo, de dados para *login* e senhas de acesso. Há plataformas, como as IaaS, entre outras, que permitem a utilização de chaves para acesso ao conteúdo interno da *Cloud*, seja num container – *bucket* ou em VM, por exemplo.

Normalmente, as chaves privadas ficam armazenadas em arquivos com extensão *pem*, por exemplo "ipbejateste_key.pem". Esta chave foi utilizada num procedimento de teste no *Microsoft Azure*, no qual a chave pública fica guardada na *Cloud* e a privada fica na posse do utilizador.

5.1. AQUISIÇÃO VIA FERRAMENTAS *CLOUD FORENSICS*

Algumas ferramentas foram analisadas em formato de teste – *trial*, com chaves temporárias cedidas pelas próprias empresas. Os resultados foram organizados de acordo com o código de escala de cinza apresentado na Tabela 3; a Tabela 4 apresenta esses resultados, com as funcionalidades que cada ferramenta oferece.

Os testes das ferramentas ocorreram em outubro de 2020 e foram posteriormente repetidos, em abril de 2021, para verificar se havia maior eficiência ou eficácia no que não tivera êxito naquele primeiro momento.

Descrição	Representação
Ferramenta Testada	
Aquisição Positiva	
Aquisição sem Sucesso	
Resposta com base na publicidade	

Tabela 3 – Legenda Descritiva

Num momento inicial, procuraram-se as ferramentas para teste em função das características anunciadas; após uma solicitação por *e-mail*, foi feito o download dos programas de teste.

Após a apresentação das finalidades deste estudo, algumas ferramentas cederam programas de teste ou códigos de ativação temporários. Outras não cederam os programas de teste, desse modo, ficando limitada a produção da tabela abaixo com base no que foi testado, a cinza escuro, sendo que em alguns casos a informação inserida baseou-se apenas na publicidade no sítio eletrônico (em preto).

Ferramenta Artefatos	MSAB XRY *Cloud*	Evidence Center Belkasoft	Paraben E3	Evidence Center Belkasoft X	Magnet Axiom *Cloud* Capabiliites	Celebrite UFED *Cloud*
Dropbox						
Facebook						
Twitter						
Google						
i*Cloud*						
Snapchat						
Emails						
Instagram						
WhatsApp						
Amazon Alexa						
Office365						
G-Suite						
Slack						

Tabela 4 – Funcionalidades oferecidas pelas ferramentas que serão testadas

As ferramentas que não foram testadas, não o foi por falta de solicitação, mas porque as empresas não puderam disponibilizá-las ou porque, por algum motivo, não tiveram em conta o *e-mail* de solicitação.

Assim, as ferramentas testadas para aquisição em *cloud* estão expressas a seguir.

5.1.1. E3:DS da Paraben Corporation

A primeira ferramenta a apresentar pertence à Paraben Corporation, é a E3 DS *Mobile Evidence Examination*. Está direcionada para a perícia forense em multiplataformas e serve para aquisição lógica e física, além de permitir a aquisição de dados na *Cloud*. (Paraben Corporation, 2020)

A tela principal da aplicação apresenta o seguinte *layout*:

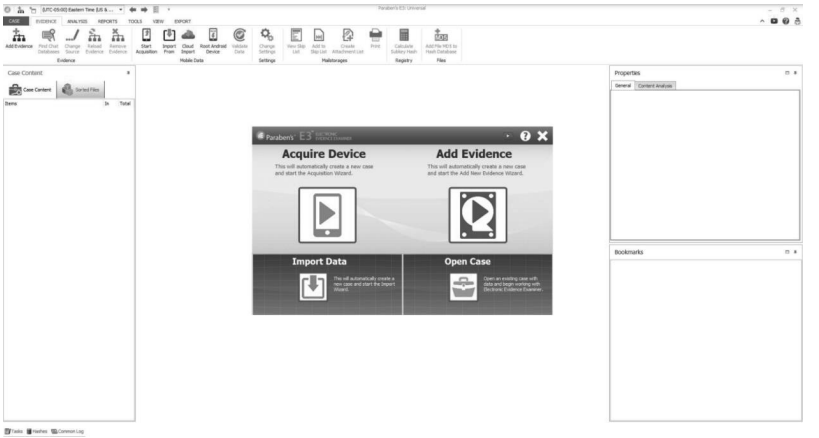

Figura 14 – Paraben Corporation Tela 1
Fonte: Paraben Corporation, 2020.

A ferramenta Paraben E3 oferece a possibilidade de aquisição diretamente a partir da *Cloud*, bastando possuir credenciais de acesso. De forma simples, basta clicar no ícone apresentado abaixo para que as opções *Cloud Import* fiquem disponíveis.

Figura 15 – Ícone do Cloud Import no Paraben

A Paraben conseguiu fazer a aquisição apenas das *Cloud* Google disponíveis na ferramenta, tendo acesso à caixa de correio eletrônico e ao Google Drive, mesmo desabilitando os controles de segurança da conta, assim também como o segundo fator de proteção apresentados nas duas figuras a seguir:

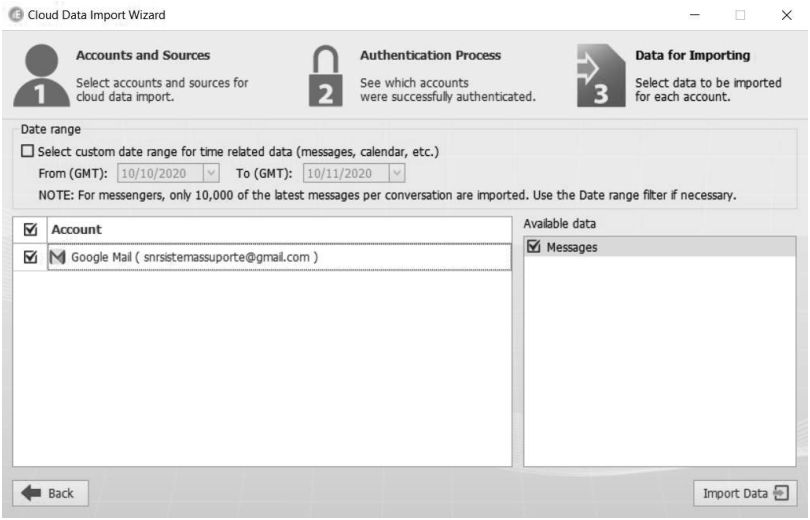

Figura 16 – Sucesso na Aquisição do Correio Eletrônico da Google

Figura 17 – Sucesso na Aquisição do Conteúdo do Google Drive

Na versão de demonstração não estava disponível a aquisição da Alexa, da Amazon, e todos os outros itens da aquisição não foram bem-sucedidos, mesmo desabilitando o segundo fator de autenticação.

Assim, mesmo apresentado uma série de recursos não foi obtida a eficiência esperada desta ferramenta, que pode ter ocorrido por não ser a versão paga da E3:DS Paraben.

5.1.2. Evidence Center da Belkasoft/Belkasoft X

A ferramenta Evidence Center da Belkasoft possui duas variantes, a normal e a versão X, que serão igualmente testadas e que apresentam várias possibilidades de aquisição em *cloud*, que foram apresentadas neste mesmo subtópico.