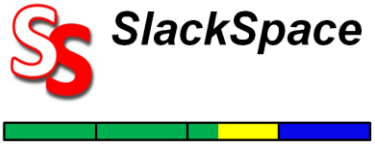


Perícia Computacional
Estudo de caso

Contexto Geral

- Esta apresentação é baseada em fatos reais e resulta de uma perícia realizada pela SlackSpace à uma empresa de médio porte na região do Triângulo Mineiro.
- Os detalhes foram retirados e algumas informações foram alteradas a fim de garantir o devido sigilo do caso.
- O objetivo desta exposição é apresentar como a Perícia pode auxiliar empresas a manter a ordem e organização; combater ilícitos; prevenir novas ocorrências por meio da devida apuração e processamento do caso; obter reparação de danos e responsabilizar os envolvidos.

O caso

- Chegaram informações para um alto executivo da área financeira da empresa X, que havia suspeita de que um gerente desta empresa estava recebendo favorecimentos indevidos de fornecedores.
- Tal executivo conversou com alguns funcionários de sua confiança e as suspeitas pareciam reais. No entanto, ele conseguiu manter o sigilo ao caso.

O caso

- Já conhecendo o portfólio de serviços da SlackSpace, tal executivo nos contatou a fim de discutir o caso. Para tal discussão ele também envolveu o coordenador da área de TI da empresa X.
- Neste caso, como já não era o primeiro serviço que a SlackSpace prestaria para a empresa X não foi preciso celebrar termo de confidencialidade, pois já havia um termo celebrado e válido fruto de trabalhos anteriores.

A reunião inicial

- Os executivos da empresa X explicaram o seguinte:
  - O suspeito era funcionário antigo e até então de muita confiança.
  - Ele era responsável pela aquisição (cotação, avaliação, compra e autorização de pagamentos) de cerca de 10 tipos de insumos utilizados pela empresa X.
  - Pelo que se suspeita ele estaria favorecendo ao menos 2 fornecedores, para cerca de 6 insumos, de modo que a empresa acabava pagando mais do que deveria.

A reunião inicial

- Em contrapartida, o suspeito estaria recebendo favorecimentos ilícitos, incluindo: viagens para sua família paga pelos fornecedores; móveis e equipamentos; além de valores monetários.
- Também foi informado que o suspeito utilizava um *notebook* e um aparelho celular da empresa, além de ter uma conta de e-mail institucional e uma área de armazenamento de arquivos em um servidor de rede.

As primeiras sugestões da SlackSpace

- Manter absoluto sigilo, não envolver mais ninguém, pois assim seria possível coletar evidências mais robustas, sem que o envolvido pudesse destruir as possíveis provas.
- Deixar que o trabalho do suspeito fosse feito normalmente.
- A SlackSpace deixou claro que sempre trabalha objetivando esclarecer a verdade e não objetiva confirmar uma tese ou suspeita, isso advém de sua imparcialidade.

As primeiras sugestões da SlackSpace

- A SlackSpace orientou que ao término dos trabalhos, poderia se chegar a um conjunto probatório que demonstrasse que o suspeito realmente praticou atos ilícitos, caso as possíveis provas apontassem para isto.
- No caso de confirmação das suspeitas, a SlackSpace deixou claro que os competentes Laudos Periciais poderiam ser usados para embasar eventual demissão por “justa causa”, ou para embasar processo de reparação na esfera cível e até processo da esfera penal.

As primeiras sugestões da SlackSpace

- A SlackSpace sugeriu que fossem feitos os seguintes exames periciais:
  - No *notebook*.
  - Na área de rede e na caixa postal do suspeito.
  - No *smatphone* (em segundo momento).
- A SlackSpace pediu 24 horas para apresentar proposta técnica e comercial.
- Posteriormente a proposta foi aceita e aprovada.

O trabalho executado

- Na primeira madrugada após a autorização da perícia, um Perito da SlackSpace esteve na empresa X (devidamente autorizado pelo executivo da área financeira) e efetuou um "clone" do disco rígido do *notebook* do suspeito. Para isso foi usado equipamento forense específico, que garante a integridade do material a ser examinado, bem como a cadeia de custódia da prova.
- Na mesma ocasião, enquanto a cópia era feita, foram feitos "*dumps*" da área de armazenamento de rede utilizada pelo suspeito e também de sua caixa postal.

O trabalho executado

- Todos os procedimentos foram executados com o devido rigor técnico-científico de modo a garantir a integridade e validade das eventuais provas obtidas a partir destes materiais coletados.
- Nada foi alterado no e-mail, na rede ou mesmo no *notebook*, de modo que o suspeito não pudesse perceber qualquer ação no dia seguinte.

O trabalho executado

- Já nas dependências da SlackSpace, os três materiais coletados (imagem no *notebook* e *dump* da área de rede e da caixa de e-mail) foram processados e indexados. Os arquivos e registros apagados também foram recuperados.
- Após o processamento, e com o entendimento do caso, um Perito da SlackSpace analisou todas as informações e chegou há algumas conclusões iniciais.

Primeiras conclusões: caixa de e-mail

- No e-mail institucional haviam milhares de mensagens trocadas entre o suspeito e dezenas de fornecedores acerca de dezenas de insumos usados pela empresa; no entanto, nenhuma mensagem que comprovasse eventual ilícito foi encontrada.
- Apenas algumas mensagens do tipo "*te mandei no WhatsApp*" ou "*sobre isso falaremos no Skype mais tarde*".
- Esse tipo de mensagem foi encontrada com três fornecedores distintos.

Primeiras conclusões: área de rede

- Na área de rede haviam milhares de arquivos diversos que variavam de arquivos pessoais a arquivos da empresa com ou sem relacionamento com as compras.
- Ainda assim foram encontradas centenas de pedidos de cotações, propostas comerciais, negociações, autorizações de compras e autorizações de pagamentos.

Primeiras conclusões: área de rede

- Dentre os arquivos previamente apagados e que foram recuperados, foram encontradas cerca de 90 propostas comerciais; e quando analisados o conjunto de arquivos, pode-se constatar que foram recebidas propostas com valores menores do que as efetivamente aprovadas e que foram sumariamente apagadas e desconsideradas.
- Esse fato foi uma primeira evidência que algo fora do padrão existia, mas por si só não seria robusta o suficiente para provar o dolo do suspeito.

Primeiras conclusões: *notebook*

- Primeiramente foram inspecionados os arquivos armazenados no *notebook* e aqueles que foram previamente apagados e recuperados.
- Nesta análise, além de milhares de arquivos relacionados ao trabalho e que não levantariam suspeitas; haviam centenas de arquivos (a maioria apagados) com propostas com valores menores e com cobranças de alguns fornecedores porque não prosseguiram no processo.

Primeiras conclusões: *notebook*

- Ainda no *notebook* foram inspecionados registros que incluíam:
  - Histórico, favoritos, termos pesquisados, autopreenchimento, senhas salvas e outros registros dos navegadores utilizados.
  - Registros de logs do sistema e de aplicações.
  - Análise de aplicativos instalados e executados.
  - Recuperação e análise de logs de aplicativos.

Primeiras conclusões: *notebook*

- Em análise aos registros do aplicativo Skype, foram recuperadas quase duas mil mensagens de texto, além de centenas de registros de ligações.
- Todas as informações de conta e da execução do aplicativo foram coletadas e preservadas de modo a validar as provas posteriormente obtidas.
- Por meio da análise destas mensagens foi possível entender um primeiro esquema ilícito:

Primeiras conclusões: *notebook*: primeiro esquema

- O fornecedor 1 era avisado pelo suspeito das condições e valores das demais propostas recebidas e era acertado o esquema ilícito, tudo pelo Skype.
- Neste caso o suspeito excluía uma ou duas propostas de outros fornecedores com valores mais baixos e os retirava com alguma informação indevida (fora do prazo por exemplo) ou mesmo sem qualquer explicação.
- Posteriormente o fornecedor 1 colocava sua proposta com valor ligeiramente abaixo dos demais fornecedores que restaram no processo e remunerava o suspeito de alguma forma.

Primeiras conclusões: *notebook*: primeiro esquema

- Foram coletadas evidências que demonstram claramente o esquema e também os exemplos do que o suspeito recebeu.

"...pois é o J****ar colocou uma proposta muito boa, ficou só em 3 a unidade e a R******la fez a 3.5 cada, depois disso sobrou o F****do e o Ca*****o com 4.5 e 5 a unidade"

"blz dá pra tirar essas duas e eu ponho a 4.4 ?"

"... ai fica bom e nesse volume solicitado consigo te ajeitar com aquele h*********er completinho..."

"... pode mandar que dou meu jeito aqui."

Primeiras entregas

- Outras evidências menos contundentes foram identificadas, e também foram incluídas no caso pois auxiliaram na comprovação da fraude continuada e rotineira.
- Foram gerados 3 Laudos Periciais, um para a caixa de e-mail, outro para a área de rede e outro para o *notebook*.
- O trabalho foi apresentado ao executivo da área financeira e os Laudos entregues, neste momento o setor jurídico foi envolvido no caso e decidiu-se pela demissão por justa causa.

Primeiras entregas

- A SlackSpace orientou para que o celular corporativo fosse retido no exato momento da demissão pois poderiam haver outras relevantes evidências no aparelho.
- No momento da demissão, o suspeito negou tudo, se declarou como inocente, que as suspeitas eram fofoca e em atitude até hostil não entregou o celular imediatamente, pois alegou ter informações de sua vida privada no mesmo, saiu andando com o celular em mãos e só depois de alguns minutos manipulando-o o entregou mas ainda se recusou a fornecer a senha de acesso ao aparelho.

Exame no celular

- O *smartphone* foi entregue a SlackSpace, que utilizando equipamento forense específico para exames periciais em dispositivos móveis procedeu com a quebra da senha e posterior extração de toda a memória do aparelho, *simcard* e cartão de dados do aparelho examinado.
- Após a extração, as informações foram processadas por meio de *software* específico e a análise foi iniciada.
- Logo no início percebeu-se que a base do aplicativo WhatsApp havia sido apagada e o aplicativo desinstalado. Os demais dados e aplicativos estavam intáctos.

Exame no celular

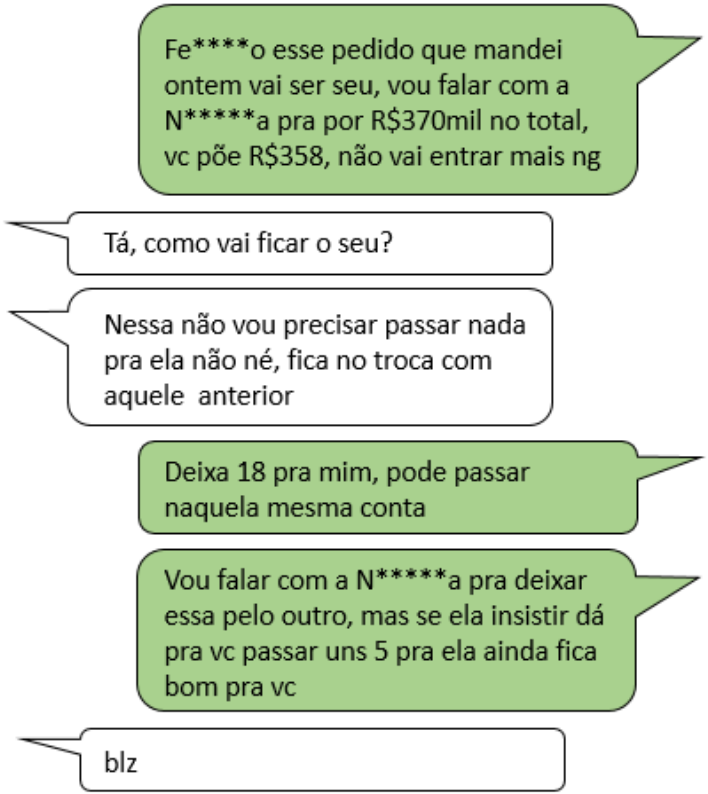
- Após análise dos demais aplicativos, registros e logs bem como dos arquivos armazenados no *smartphone,* nada de interesse foi encontrado.
- Procedeu-se então a recuperação da base de dados no aplicativo WhatsApp e neste caso a recuperação foi completa e todos os registros foram recuperados.
- Em análise detalhada das conversas e arquivos trocados pelo WhatsApp, ficou claro a existência de um segundo esquema, envolvendo outros dois fornecedores.

Exame no celular

- Neste segundo esquema ilícito, envolvia a aquisição de insumos mais específicos, e era comum a existência apenas de dois a três fornecedores, até mesmo pela forma como solicitação de cotação era feita.
- O suspeito mantinha contato com dois fornecedores, que operavam em formado de cartel, sob o comando do suspeito. Eram acertados os valores a serem apresentados, e além da intercalação dos vencedores havia repasse entre os fornecedores a fim de compensar a perda de um em relação ao outro numa compra maior e vice e versa.

Exame no celular

- Ainda neste esquema o suspeito garantia a retirada de eventual proposta com valor menor e recebia valores monetários de ambos os fornecedores.
- Foram encontrados centenas de registros no WhatsApp que comprovaram o esquema, alguns exemplos são mostrados:


Fe****o esse pedido que mandei ontem vai ser seu, vou falar com a N*****a pra por R$370mil no total, vc põe R$358, não vai entrar mais ng
Tá, como vai ficar o seu?
Nessa não vou precisar passar nada pra ela não né, fica no troca com aquele anterior
Deixa 18 pra mim, pode passar naquela mesma conta
Vou falar com a N*****a pra deixar essa pelo outro, mas se ela insistir dá pra vc passar uns 5 pra ela ainda fica bom pra vc
blz

Conclusão

- O Laudo do celular foi entregue e um conjunto probatório robusto e válido foi gerado, validado e preservado pelos Laudos.
- Soube-se depois que a empresa ingressou com processo judicial na esfera penal. Foi pedido à autoridade policial que solicitasse ao juízo à concessão de mandados de busca e apreensão na residência do suspeito e na sede dos três fornecedores envolvidos. Em paralelo foi ajuizado pela a empresa X processo na esfera cível para a reparação de danos.

Se a SlackSpace não tivesse sido envolvida:

Como poderia ter sido diferente

- A empresa X, até por seu porte, tem uma área de TI e tem profissionais que poderiam auxiliar seus executivos na verificação deste caso; porém certamente a empresa passaria por alguns problemas:
- O devido sigilo não seria mantido.
- Não se teria a necessária imparcialidade e todos os resultados seriam de pouca valia em processos judiciais e certamente seriam questionados pela outra parte em decorrência de conflito de interesses.

Se a SlackSpace não tivesse sido envolvida :

Como poderia ter sido diferente

- A prova não seria devidamente preservada e validada, o que poderia colocar tudo a perder.
- Não seriam obtidos os mesmos resultados pela ausência de experiência na área forense e por não ter as ferramentas e equipamentos adequados à disposição dos profissionais.
- Não seria possível acessar as informações do *smartphone* pelo não fornecimento da senha e também não seria possível recuperar as bases de dados do WhatsApp, ou seja, o segundo esquema provavelmente não seria descoberto.

SlackSpace

Recuperação de Dados
Perícia Computacional
Testes de Penetração

contato@slackspace.com.br
34 99861 5111 – 34 3232 5111

www.slackspace.com.br
Rua República da Síria, 68A
Uberlândia – MG – CEP 38405-070