



SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA CIENTÍFICA
INSTITUTO DE CRIMINALÍSTICA
SEÇÃO DE COMPUTAÇÃO FORENSE

PROJETO CIÊNCIAS FORENSES NAS ESCOLAS
Diálogos de conscientização para uso responsável de computadores e dispositivos de armazenamento de dados por crianças e adolescentes

A Sessão de Computação Forense do Instituto de Criminalística do Paraná atua em perícias em dispositivos de armazenamento computacionais (celulares, discos rígidos de computadores e notebooks, tablets, cartões de memória, entre outros) quando há indícios de que neles se encontram armazenados dados que possam comprovar a autoria e modus operandi de um delito. Entre os casos que estes peritos analisam há homicídios, suicídios, tráfico de drogas, falsificação de documentos, recuperação de imagens de câmeras de segurança, crimes contra o patrimônio público, estupro, e casos envolvendo crianças e adolescentes. Todos estes casos são atendidos através de ofícios de autoridades policiais, judiciais, administrativas e correccionais.

O trabalho dos peritos vem evoluindo ano após ano e hoje há diversos recursos disponíveis nos laboratórios de Computação Forense da Polícia Científica do Paraná que permitem a realização dos exames em equipamentos de forma completa resultando em uma melhor resposta às autoridades solicitantes. Os peritos recuperaram históricos em aplicativos de conversação (“chats”) em celulares ou outros meios como computadores e tablets, inclusive informações apagadas, entre outros dados importantes para as autoridades elucidarem os crimes. São inúmeros os casos em que a perícia de computação forneceu informações suficientes para a completa elucidação de crimes.

No ano de 2014 foi percebida uma mudança no perfil de exames solicitados aos laboratórios de Computação Forense do Instituto de Criminalística do Paraná: o aumento de casos relacionados a crianças e adolescentes ocasionados pelo mau uso de recursos computacionais. São casos que vem preocupando os peritos da área e que apresentam características similares entre si, pois envolvem imagens ou vídeos de jovens em situações de nudez, com o envio deste material para pessoas ou grupos de pessoas através de aplicativos como o Facebook e de conversação como o WhatsApp e SnapChat.

Como estes arquivos são encaminhados para diversos outros contatos, a replicação do material cria uma rede de pessoas que conhecem e compartilham estes conteúdos, consistindo em crime de violência previsto no Estatuto da Criança e do Adolescente (ECA). Além de se tratar de crime, há casos em que esta exposição das imagens dos jovens resultam em consequências graves que vão desde a perseguição pelos colegas do jovem que teve sua intimidade compartilhada até mesmo a casos de suicídio, como vem sendo divulgado na mídia.

Preocupados com este e outros perfis de uso que podem oferecer riscos às pessoas e entendendo que a realidade enfrentada diariamente pelos peritos criminais é muito diferente daquela em que vive a maioria da população, peritos do Instituto de Criminalística iniciaram trabalhos em escolas buscando informar e conscientizar crianças, jovens, pais, professores, enfim, a população em geral dos perigos que este tipo de prática pode trazer para uma família. A abordagem é realizada através de palestras onde os peritos descrevem situações que podem colocar em risco as famílias, quais são os riscos que os jovens correm ao compartilhar imagens ou vídeos com conteúdo impróprio, bem como indicam algumas práticas saudáveis para melhorar o perfil dos usuários de recursos computacionais, sempre discutindo casos analisados pelos laboratórios de Computação Forense ou casos de repercussão na mídia onde o mau uso foi verificado.

As palestras em escolas são realizadas com grupos de alunos divididos por faixa etária, pois a abordagem para os mais novos é feita de maneira diferente daquela empregada para os mais velhos. As turmas são divididas em 6º ao 7º ano, 8º e 9º ano e Ensino Médio (o 3º ano, preferencialmente, é separado dos demais). Os pais dos alunos são convidados a assistir a palestra sem os filhos, depois das palestras com os alunos, pois este modelo apresenta maior retorno dos jovens, que se sentem intimidados pela presença dos pais e não interagem com os peritos quando estão na presença desses.



SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA CIENTÍFICA
INSTITUTO DE CRIMINALÍSTICA
SEÇÃO DE COMPUTAÇÃO FORENSE

Em todas as palestras os peritos descrevem a estrutura da Secretaria de Segurança Pública no Paraná, informando o que é a Polícia Científica, como está dividida e onde atua. A função do perito criminal do Paraná é descrita, assim como os trabalhos periciais realizados nos Institutos de Criminalística do Paraná, fornecendo uma breve visão de todas as seções.

As principais categorias de casos encaminhados aos laboratórios de Computação Forense são listadas e para algumas delas os peritos citam boas práticas que podem impedir que estes crimes aconteçam ou mesmo que possam auxiliar um eventual exame pericial em um dispositivo de armazenamento.

Descreve-se, também, quais são os principais crimes envolvendo crianças e adolescentes e que vestígios podem ser obtidos em meios de armazenamento computacionais, discutindo-os com certo detalhamento, com exemplos reais e com casos de conhecimento dos peritos que foram divulgados na mídia.

As crianças até o 7º ano são abordadas de forma simples e sem o uso de termos como pedofilia, estupro ou outros termos que podem não ter sido ainda apresentados a elas por seus pais ou responsáveis. A abordagem trata dos riscos de exposição em redes sociais, aliciamento através de chats de jogos, cuidados com comentários em redes sociais ou aplicativos de conversação, a extensão que o cyberbullying pode ter, o perigo das conversas na rede com desconhecidos, cuidados com o conteúdo visualizado, além da importância de sempre recorrer a algum adulto responsável por eles quando alguma situação diferente ou suspeita durante a navegação na rede ocorrer.

Aos jovens do 8º ano e Ensino Médio o mesmo conteúdo abordado para as crianças é discutido, entretanto, os termos pedofilia, estupro, homicídio, entre outros, são utilizados de forma direta e sempre buscando causar um impacto positivo nos jovens. Por exemplo, quando se trata de pedofilia, o termo é usado quando os peritos discutem casos como aqueles em que pedófilos obtêm imagens de jovens nus na rede social Facebook ou outros meios computacionais e usam estas mesmas imagens em sites de pedofilia.

Para as palestras nenhum material de apoio é utilizado, pois o modelo de conversa tem sido mais aceito por eles, permitindo uma maior interação perito-aluno-pais. Em diversos momentos as conversas são guiadas pelas perguntas da plateia e como nossa experiência mostra que em turmas grandes os alunos se sentem mais confiantes e fazem mais perguntas, sempre solicitamos que sejam agrupadas diversas turmas para cada palestra (temos experiência em turmas de até 400 alunos).

O mais interessante nas palestras com os pais é o retorno que fornecemos a eles, contando o que foi discutido nas conversas com as crianças e jovens, pois assim eles passam a ter conhecimento do que está acontecendo naquele meio onde seu filho está inserido.

Em resumo, a proposta é a realização de conversas abertas dos peritos com os jovens sobre o que está acontecendo na esfera criminal quando ocorre mau uso de recursos computacionais, buscando mostrar que estamos atentos e preparados para descobrir uma quantidade muito grande de informações armazenadas em dispositivos computacionais e que poucos conseguem esconder um crime em meio virtual dos profissionais da perícia. Espera-se, assim, fazer com que os jovens pensem melhor antes de fazer algo com seus tablets, celulares e computadores, pois as consequências podem ser graves, mesmo para crianças e jovens abaixo dos 18 anos. E para os pais e professores permitimos o conhecimento daquilo que as crianças e jovens estão fazendo, seja através dos casos expostos pelos peritos ou pelos comentários e questionamentos dos alunos durante as palestras.

PORNOGRAFIA INFANTIL

Pornografia infantil praticada por menores é crime?

Pornografia infantil de menor para menor é ATO INFRACIONAL (passível de punição com medidas socioeducativas): O Estatuto da criança e do adolescente (ECA) não prevê em



SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA CIENTÍFICA
INSTITUTO DE CRIMINALÍSTICA
SEÇÃO DE COMPUTAÇÃO FORENSE

seus artigos que o abuso de menores só é delito quando praticado por uma pessoa com maioridade penal. Há punições previstas para menores assim como há para adultos. Para os menores de idade as medidas socioeducativas vão desde advertência, prestação de serviços sociais até o internamento, onde jovens são abrigados em lares de recuperação de menores infratores). Mesmo em crimes virtuais!

Há casos divulgados na mídia de punições ou mesmo de pagamento de indenizações por menores infratores após estes atingirem a maioridade (quando o caso só é julgado após alguns anos da queixa). Exemplo é o caso de um casal que filmou uma relação com 17 anos, com consentimento de ambos e o rapaz após o término do namoro divulgou o vídeo da rede mundial de computadores. Ele pagou, com 21 anos, indenização à ex-namorada no valor de 30mil.

A tipificação dos crimes que envolvem pornografia infantil no ECA envolvem a Produção, o armazenamento e o compartilhamento de imagens e vídeos envolvendo menores em situações de sexo ou que simulem sexo. Até mesmo desenhos que tenham o mesmo conteúdo são enquadrados nesta lei.

Como procuramos vestígios que envolvem pornografia infantil em materiais encaminhados para exame?

Procuramos por imagens, vídeos, conversas em aplicativos, compartilhamento de arquivos por aplicativos como Torrent, Ares, entre outros específicos para compartilhamento de arquivos. E quando encontramos buscamos sempre saber de onde esta imagem veio e se foi compartilhada com alguém e por qual meio, de maneira a tipificar o crime (como está descrito acima). Conseguimos mapear aplicativos utilizados, contas utilizadas, dispositivos como pendrivers conectados a computadores, entre outros itens importantes para que seja realmente “contada a história” daqueles conteúdos e seu caminho na rede;

Para facilitar o trabalho de busca por imagens de pornografia infantil utilizamos um banco de hash de fotos de pornografia infantil por polícias do Brasil e exterior. Este banco de dados é alimentado com novas imagens de casos que fazemos diariamente; Possuímos ferramentas que permitem a recuperação de dados apagados quando estes não foram sobrepostos por outra informação.

Fotografias possuem alguns dados importantes para a perícia, que podem fornecer desde a data e hora da tomada fotográfica até localização GPS de onde esta foi obtida, marca, modelo e algumas vezes até mesmo número de série dos equipamentos utilizados para obter as imagens.

Há casos em que é possível a obtenção dos dados mesmo em equipamentos danificados e há outros em que as ferramentas que utilizamos não permitem que os dados sejam obtidos. Portanto, não são todos os casos que conseguimos resolver, mas há alguns que podem parecer casos perdidos em que recuperamos muitas informações importantes para a investigação.

Quais são os principais casos que trabalhamos envolvendo pornografia infantil?

Casos recebidos por denúncias onde foi relatado que menores estavam sofrendo abusos e outros onde relatam que alguém viu imagens e vídeos nos equipamentos dos



SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA CIENTÍFICA
INSTITUTO DE CRIMINALÍSTICA
SEÇÃO DE COMPUTAÇÃO FORENSE

denunciados;

Casos onde fotos e filmes de menores foram compartilhados na rede mundial de computadores (NUDES). Nestes casos, na maioria das vezes, verificamos que o compartilhamento das imagens foi iniciado pelas próprias “vítimas”, que normalmente têm entre 13 e 14 anos e são meninas. Estas meninas enviaram fotos ou mesmo abriram suas câmeras para namorados que insistiram ou não para que a namorada enviasse estes conteúdos. Após o envio ou término da relação os meninos compartilham as imagens e vídeos em grupos do WhatsApp e aplicativos como SnapChat, gerando problemas sérios às famílias das vítimas que acabam por denunciar os crimes.

DEEPWEB

O que é a DeepWEB?

Conhecida como o submundo da internet, esta rede de equipamentos possibilita aos seus usuários (normalmente usuários do aplicativo Tor), visualizarem e compartilharem informações sem controle algum de conteúdo (o google controla o que é indexado em seus servidores, filtrando conteúdos contra a lei e até mesmo algum ofensivos). Esta rede também promete que os seus usuários sejam anônimos, isto é, que suas identidades virtuais não sejam reveladas.

Nesta rede há desde trabalhos acadêmicos, fóruns interessantes de discussão de estudos ao redor do mundo, até segredos de governos, conteúdos de pornografia infantil, matadores de aluguel que postam vídeos mostrando que realmente fazem o serviço, experiências com humanos, comércio de vários produtos ilegais (armas, drogas, até mesmo green cards), entre outros diversos assuntos que não são facilmente encontrados em buscadores na rede www.

A DeepWEB é mesmo anônima?

Polícias do mundo já conseguiram desvendar redes de criminosos na deep web e outras redes deste tipo. É difícil, depende-se muito tempo e muito processamento de dados para que estas redes sejam desvendadas, mas isto não é impossível; Assim como o google traça os nossos perfis de uso (usando dados como nossas pesquisas google, google maps, vídeos do youtube, entre outros aplicativos, sempre buscando clientes em potencial para os produtos que anuncia), há a possibilidade de se traçar o perfil de um usuário da deepweb. Há casos em que crianças estão brincando de acessar conteúdos indevidos nesta rede e relatos de policiais acabaram por fazer busca e apreensão em algumas casas em busca de armas ou outras provas de terrorismo após análise de um perfil na deepweb. Lembrando que uma conexão de computador, celular, entre outras, podem fornecer dados que nos levam às casas de suspeitos (endereços reais podem ser atrelados a endereços virtuais).



SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA CIENTÍFICA
INSTITUTO DE CRIMINALÍSTICA
SEÇÃO DE COMPUTAÇÃO FORENSE

O que são as palestras em escolas que a Polícia Científica do Paraná realiza?

São conversas onde casos são comentados e discutidos, sempre procurando informar alunos, pais e professores sobre os perigos, possíveis consequências e, claro, do potencial das polícias especializadas na busca de informações e provas sobre crimes virtuais.

O que mais atrai a atenção dos alunos nas palestras em escolas?

Quais aplicativos podem ter seus dados recuperados quando apagados;

O que são as medidas socioeducativas e o que pode acontecer com eles quando cometem um ato infracional;

Se quando alguém armazena um nude de uma criança ou adolescente isto também configura crime ou ato infracional (mesmo quando a própria “vítima” faz a foto e compartilha);

A deepweb é mesmo anônima?

Porque não posso invadir o computador ou jogo do meu amigo se for só por brincadeira?

Como faço para me tornar perito?

ALGUMAS DICAS INTERESSANTES:

- Não confie em tudo o que está na rede:

Não acredite em qualquer postagem. Você pode compartilhar uma mentira e sofrer consequências na área civil.

- Não deixe que estranhos entrem na sua casa:

Não compartilhe imagens e vídeos que mostrem o que há dentro da sua casa.

Procure fazer vídeos (youtubers, aplicativo musicaly) em locais onde há paredes sem objetos ao fundo. Algumas informações são obtidas através de objetos pessoais (por exemplo, um livro ou um brinquedo pode ser o suficiente para o início de uma conversa com um novo amigo em uma rede social ou um jogo, sem que você saiba que ele pesquisou sua vida antes e não é apenas alguém que gosta das mesmas coisas que você).

- Não entre na casa de estranhos:

Algumas crianças estão brincando de invadir computadores e jogos de amigos (hackear) e isto pode ser considerado crime dependendo das informações que foram obtidas ou mesmo dos danos provocados no equipamento “atacado”. Há também o risco de uma invasão ser realizada por um hacker profissional coincidente com a invasão brincadeira de uma criança. Como os hackers costumam limpar os vestígios de forma a não deixar dados suficientes que permitam sua captura e crianças apenas brincam deixando diversos vestígios, a probabilidade da perícia apontar para a invasão da criança como sendo a única existe.

Em todas as escolas visitadas nas palestras que realizamos há relatos de jovens que invadem câmeras de celulares de amigos para obter imagens dos amigos em



SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA CIENTÍFICA
INSTITUTO DE CRIMINALÍSTICA
SEÇÃO DE COMPUTAÇÃO FORENSE

situações constrangedoras, na maioria das vezes por brincadeira. Mas é muito estreito o limite entre o que é ou não crime. Uma ofensa para uma pessoa pode ser levada na brincadeira, para outra não. Uma imagem de uma menina tomando banho pode afetar uma jovem de uma maneira, mas há casos de suicídio.

- Não converse com estranhos:

Procure saber com quem você se comunica em aplicativos como aqueles de namoro, em redes sociais como facebook ou mesmo em jogos on-line. Nos jogos crianças não têm noção de que existem perfis falsos e se comunicam com adultos pensando serem crianças. Estes adultos procuram se tornar amigos dos jogadores conversando sobre dados obtidos em redes sociais das crianças (fotos no instagram, por exemplo), buscando sua confiança.

- Não revele dados importantes sobre sua vida pessoal:

Procure não fazer check-in nos locais onde vai, principalmente em aeroportos ou rodoviárias, pois assim você, além de contar onde está revela que não está na sua casa, por exemplo. Um sequestrador de Santa Catarina revelou, quando foi capturado, que utilizou dados de check-in dos pais para saber a melhor hora de sequestrar seu filho;

Cuidado com informações sobre hoje é dia de fazer isto, sábado farei aquilo, marcar encontros com amigos em posts do facebook, por exemplo. Você conta sua rotina, algo extremamente complicado para um ladrão ou sequestrador mapear apenas seguindo seus passos na vida real.

Estamos fornecendo informações de graça aos bandidos que antes eram difíceis de se obter (antes isto era feito na porta das escolas, vigiavam nossos passos). Hoje um alvo pode ser escolhido na rede mundial de computadores ou através de uma rede social pelo simples fato de ser fácil traçar sua rotina e, claro, por esta pessoa mostrar em fotografias o que possui de bens ou seu poder aquisitivo através de fotos de viagens, passeios e lugares que frequenta.

- Cuidado com seus acessos:

Há casos em que as pessoas acessam apenas pornografia adulta, mas com a participação de jovens que parecem adolescentes. Nestes casos relatamos que se trata de conteúdo com possíveis adolescentes. É preciso ter cuidado com os conteúdos que são acessados de pornografia para que não se crie um perfil indevido com imagens e vídeos de possíveis adolescentes.

O google e até mesmo a deep web criam perfis de uso de seus usuários (na deep web isto é muito difícil, mas pode acontecer), então cuide dos seus acessos. Não procure conteúdos indevidos com frequência, seja por brincadeira ou por interesse pessoal mesmo, pois você pode passar a ter o perfil errado no mundo virtual, e ter que responder por isto, tanto para a polícia, como para os “donos” dos conteúdos. Já imaginou um vendedor de armas querendo saber quem é este usuário que está sempre pesquisando seus “produtos”?



SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA CIENTÍFICA
INSTITUTO DE CRIMINALÍSTICA
SEÇÃO DE COMPUTAÇÃO FORENSE

Em resumo, nós defendemos que o que falta é orientação. É preciso conversar com as crianças e jovens e para isto não é necessário saber como este ou aquele aplicativo funciona. Precisamos continuar fazendo o que nossos pais faziam quando éramos crianças, nos ensinando o básico que nos serviu de lição para tudo:

- Não confie em tudo o que você vê ou te contam;
- Não deixe que estranhos entrem na sua casa;
- Não entre na casa de estranhos;
- Não converse com estranhos;