DOI: 10.5769/C2015007 or http://dx.doi.org/10.5769/C2015007

Investigação em Ambientes de Jogo Multijogadores *Online*

Juliano K. M. Oya, Cleber Scoralick Junior e Bruno W. P. Hoelz

Resumo—**Jogos *online* por meio da *Internet* podem ser utilizados para auxiliar ou cometer crimes como exploração sexual de crianças e adolescentes, racismo, injúria, difamação, calúnia e associação criminosa. Além disso, crimes praticados fora do ambiente *online*, como furtos, podem apresentar vestígios inesperados nesse ambiente. Neste trabalho, realizou-se um estudo exploratório do ambiente de jogos *online* e definiu-se uma metodologia para a investigação de crimes nesse mesmo ambiente. A metodologia proposta, baseada na análise de tráfego de redes e na identificação de endereços IP, foi aplicada em um estudo de caso real, no qual foi possível estabelecer com sucesso a autoria do crime.**

Palavras-Chave—crimes cibernéticos, análise de tráfego de redes, jogos online.

Abstract—**Online games over the Internet have been increasingly used to aid or commit crimes such as child exploitation, racism, slander, defamation, and crime association. In addition, crimes committed offline, such as theft, can present unexpected traces in the online world. In this work, we carried out an exploratory study of an online gaming environment and set up a methodology for the investigation of crimes in such environments. The proposed methodology, based on network traffic analysis and identification of IP addresses, was applied in a real case study, in which it was possible to successfully establish the authorship of the crime.**

Keywords—cyber crime, network traffic analysis, online games.

I. INTRODUÇÃO

A análise de tráfego de redes é uma atividade que consiste no uso de *hardware* e *software* para a coleta e análise do tráfego de mensagens de protocolos de rede, como o TCP, UDP e IP. É, geralmente, realizada por administradores de redes para detectar anomalias na rede; encontrar pontos de bloqueios na rede; descobrir equipamentos e cabeamentos defeituosos; observar importantes mensagens não mostradas pelas aplicações; detectar falhas de segurança, instalação ou *bugs* em serviços disponíveis na rede; e descobrir o tráfego "pirata" dentro da rede [7].

Por meio da análise de tráfego de redes é possível investigar os ambientes virtuais de jogos eletrônicos, também conhecidos como jogos multijogadores *online*. Nesse tipo de ambiente a interação entre os usuários (ou jogadores) ocorre, em nível de aplicação, por meio da troca de mensagens e comandos. Cada usuário, dentro desse mundo virtual, é representado por um *nickname* ou um *avatar*, os quais podem ter pouca relação com os verdadeiros nomes reais de cada usuário.

Ambientes virtuais baseados na *Internet* são cada vez mais utilizados para auxiliar ou cometer crimes [3] como exploração sexual de crianças e adolescentes, racismo, injúria, difamação, calúnia, formação de quadrilha, entre outros. Além disso, crimes praticados fora do ambiente *online*, como furtos, podem apresentar vestígios inesperados nesse ambiente.

Apesar do anonimato criado pelo uso de *nickname* ou *avatar*, é possível identificar o usuário por meio da análise das mensagens dos protocolos TCP, UDP e IP. Cada interação entre os usuários de um ambiente virtual gera um conjunto de segmentos TCP e UDP que são encapsulados em pacotes IP [1].

Neste artigo, é proposto um método de trabalho para a coleta e análise de dados de tráfego de rede com o objetivo de identificar possíveis autores de um delito por meio do endereço IP. Assim, serão apresentadas as atividades que constituem o método de trabalho, quais sejam: preparação do ambiente de coleta, coleta de dados de tráfego de redes, análise dos dados coletados e finalmente a preparação de um relatório para a autoridade competente.

Este trabalho é divido em três seções:

a) Referencial teórico, na qual são apresentados os conceitos relacionados aos ambientes de jogos multijogadores *online*, os vestígios digitais e a identificação de autoria por meio de endereços IP;

b) Metodologia, na qual são descritos os instrumentos e procedimentos e é apresentado o estudo de caso no qual o método de investigação é aplicado;

c) Conclusão, na qual são discutidos os resultados obtidos e os possíveis trabalhos futuros..

II. REFERENCIAL TEÓRICO

Este tópico apresenta os fundamentos relacionados às técnicas, ferramentas e conceitos envolvidos na investigação em ambientes de jogo multijogadores *online*. A *Seção A* descreve os ambientes de jogo multijogadores *online*. A *Seção B* descreve o procedimento para a identificação de autoria por meio de endereços IP.

A. Ambientes de jogo multijogadores online

Mcshaffry e Graham [6] apresentam um modelo lógico da arquitetura geralmente utilizada pelos sistemas de jogos. Na Figura 1, são apresentados os principais módulos e interfaces que compõe esse modelo.

Como os mesmos autores explicam, a camada de aplicação se preocupa com a máquina na qual o jogo é executado. Nesta

camada é onde estará localizado o código que realiza a comunicação com dispositivos de *hardware* (como o *mouse*, o teclado e o monitor), serviços do sistema operacional (tais como as comunicações de rede) e operações como a inicialização e desligamento do jogo.

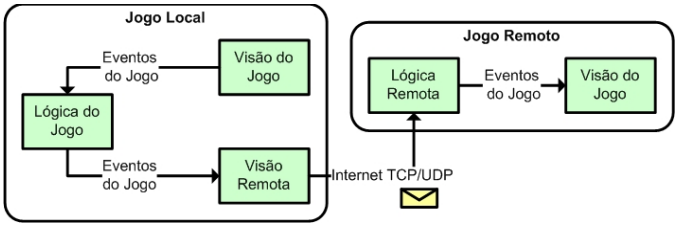

Fig. 1. Visão geral de uma arquitetura lógica de um jogo.
Fonte: Adaptado de Mcshaffry e Graham [6].

Na camada de lógica, ainda segundo Mcshaffry e Graham [6], é possível encontrar os subsistemas de gestão de estado do jogo, que é responsável por comunicar as mudanças de estado para outros sistemas, assim como aceitar comandos de entrada de outros sistemas. A camada de visão do jogo é responsável por apresentar o estado do jogo e traduzir entrada em comandos de jogo que são, então, enviados para a lógica do jogo. Por fim, a camada de visão remota é responsável por enviar, em jogos que utilizam a rede de computadores, dados de sincronização entre o jogo local e o jogo remoto.

Esse modelo de arquitetura é utilizado na grande maioria dos sistemas de jogos, assim como para os modelos de interação entre os jogadores e o sistema de jogo apresentados por Fullerton [5], os quais são: *single player*; *player vs. player*; *multilateral competition*; *team competition*; *multilateral team competition*; *unilateral competition*; *multiple individual vs. game*; *multiple players compete against the system*; *cooperative*.

Os jogos do tipo *single player* ou *player vs. player* não utilizam, na maioria das vezes, a conexão com a *Internet* durante a execução do jogo. Já os jogos do tipo *multiplayer* utilizam, na maioria das vezes, a conexão com a *Internet* para que os jogadores interajam entre si.

A respeito do ambiente de conexão, McShaffry e Graham [6] apresentam 5 modelos tipicamente utilizados pelos jogos atuais, que são: jogo individual sem conexão, jogo individual com conexão, jogo multijogador com conexão direta, jogo multijogador com conexão rede local, jogo multijogador com conexão *Internet*. A Figura 2 mostra graficamente a forma de organização e interconexão dos equipamentos que compõem esses modelos, sendo que em alguns casos pode haver a conexão com a *Internet* para possibilitar a troca de dados entre os jogadores. Nessa Figura, em 2-A é apresentado o modelo jogo individual sem conexão. Em 2-B são apresentados os modelos jogo multijogador com conexão direta e jogo multijogador com conexão rede local. Em 2-C é apresentado jogo individual com conexão *Internet*. Por fim, na Figura 2-D, é apresentada uma arquitetura híbrida de comunicação, na qual os jogadores se comunicam entre si e também com um servidor central de jogo.

A técnica de análise de tráfego de rede pode ser aplicada para os modelos de conexão que envolvam múltiplos jogadores por meio de uma conexão com a rede local ou com a *Internet*, como mostrado na Tabela I. Nela são relacionados os modelos apresentados por McShaffry e Graham [6] e a possibilidade de se realizar a captura do tráfego de dados na rede.

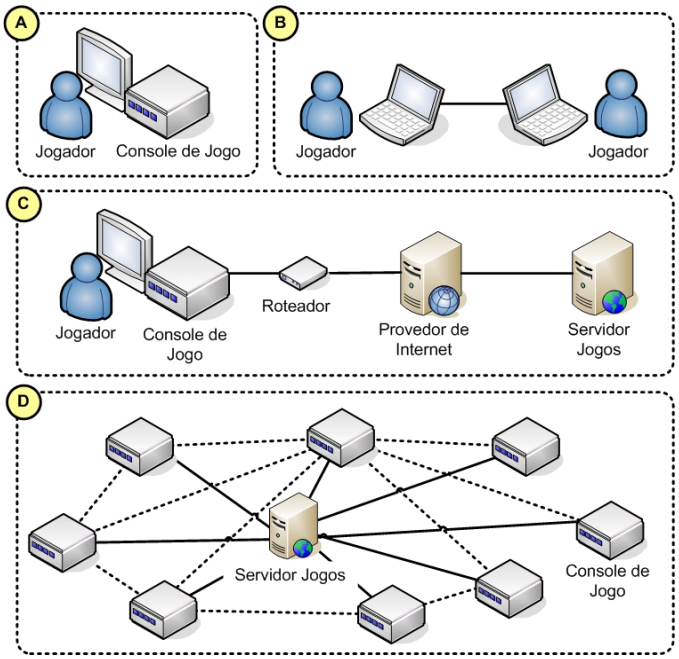

Fig. 2. Modelos de conexão dos sistemas de jogos
Fonte: Adaptado de McShaffry e Graham [6].

TABELA I. PRINCIPAIS CARACTERÍSTICAS DOS MODELOS DE CONEXÃO.

	Interação dos jogadores	Conexão com Internet	Provedor de Conexão	Servidor de Jogos	Análise de Tráfego Local	Análise de Tráfego Remota
Jogo Individual s/ Conexão	✗	✗	✗	✗	✗	✗
Jogo Individual c/ Conexão	✗	✓	✓	✓	✓	✗
Jogo Multijogador c/ Conexão Direta	✓	✗	✗	✗	✓	✗
Jogo Multijogador c/ Conexão Rede Local	✓	✗	✗	✗	✓	✗
Jogo Multijogador c/ Conexão Internet	✓	✓	✓	✓	✓	✓

O método de investigação apresentado neste trabalho é adequado para os modelos de arquitetura de jogos de Rabin [9] do tipo *multiplayer*, ou seja, para aqueles jogos que envolvem 2 ou mais jogadores interagindo entre si por meio de uma conexão de *Internet* e, ainda, sabendo-se o nome virtual do alvo e interagindo com ele.

B. . Identificação de autoria por meio de endereços IP

Os jogos multijogadores *online* utilizam o protocolo TCP/IP para a troca de dados entre os jogadores, tais como eventos de sincronização do sistema do jogo. Assim é possível utilizar a análise de tráfego de redes para extrair informações da camada de redes para identificar um possível alvo.

Na Figura 3, são apresentadas as camadas do modelo OSI [12] utilizadas para realizar a comunicação entre o sistema de jogo e os jogadores

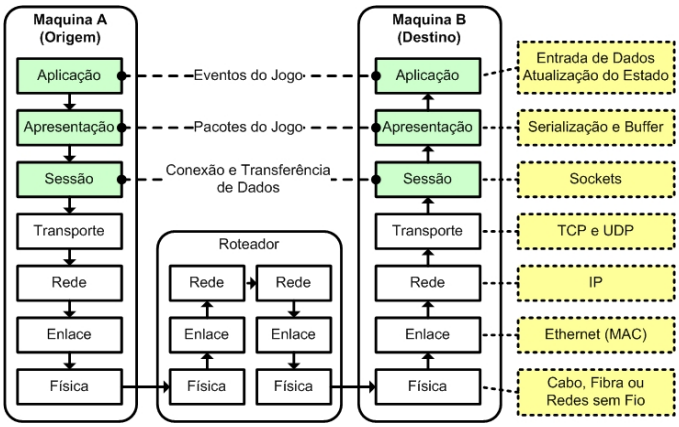

Fig. 3. Modelo OSI com as camadas de comunicação entre os jogos *online*. Fonte: Adaptado de Rabin [9].

O protocolo IP tem como principal característica a identificação única de um dispositivo de rede através de seu endereçamento. Existem duas versões do protocolo IP: IPv4 e IPv6. O IPv4 possui um endereçamento de 32 *bits* e o IPv6 utiliza um endereçamento de 128 *bits*.

Uma estratégia adotada por algumas instituições ou estabelecimentos para atenuar a escassez de endereços IPv4 é a utilização dos endereços privados de `10.0.0.0` a `10.255.255.255`, de `172.16.0.0` a `172.31.255.255` e de `192.168.0.0` a `192.168.255.255` por seus usuários. Assim, os dispositivos de rede, que utilizam esses endereços IPs, não podem comunicar-se diretamente com outros dispositivos na *Internet*, necessitando de um serviço de tradução de endereços IPs privados para endereços roteáveis na *Internet*. Comumente o serviço utilizado é o NAT (*Network Address Translation*) [11].

Para organizar o endereçamento IP, faixas de endereçamentos são distribuídos de forma hierárquica, sendo a IANA (*Internet Assigned Numbers Authority*) [17] a autoridade central responsável. No Brasil, a autoridade regional é a CGI.br [4], que, dentre outras atribuições, realiza a alocação de endereços IP no âmbito nacional.

Dessa forma, um provedor de conexão de *Internet* (também chamados de ISP – *Internet Service Provider*) deve contratar faixas de endereços IP através dos registros regionais (ou nacionais, quando houver) e, quando um cliente desse provedor se conectar à *Internet*, ele deverá receber um dos endereços IP pertencentes à faixa contratada [11].

Para poder utilizar a *Internet*, o dispositivo que interliga a rede local ao ISP deve se autenticar no provedor. O registro destas autenticações é de extrema importância para a investigação, pois através dele é possível identificar que um cliente iniciou uma conexão em determinada data e horário, qual o endereço IP recebeu, e a data e horário da desconexão. Em uma nova conexão, o mesmo usuário pode receber outro endereço IP, por isso é de suma importância que a investigação saiba, além do endereço IP, o momento exato que uma atividade ilícita ocorreu [11].

Assim, os IPs descobertos durante uma investigação estão vinculados aos ISPs, os quais podem ter sido utilizados por algum de seus clientes. Nesse caso, é necessário solicitar ao ISP qual o cliente que utilizava o endereço IP no dia e hora especificados. Essa solicitação muitas vezes é feita através de mandado judicial [8] (e que algumas vezes é precedida de uma requisição cautelar para preservar os dados de *logs*).

Da mesma forma, pode-se fazer uma solicitação para o provedor de aplicação para que o mesmo forneça os *logs* de utilização de seus serviços. Assim, o provedor de aplicação pode fornecer os dados do usuário de seus serviços como o IP e data e hora de utilização.

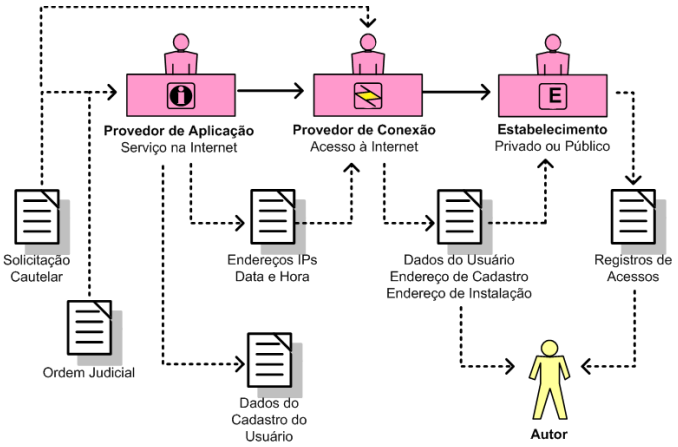

Fig. 4. Passos para verificar identificar o IP da conexão utilizada por um usuário.

Na Figura 4, é ilustrado o fluxo de informações fornecidas pelos provedores de aplicação, provedores de conexão e pelo estabelecimento. Uma solicitação cautelar de preservação de registros é feita pela autoridade policial, até que seja emitida a ordem judicial para que os provedores de aplicação e de conexão forneçam os registros de conexão (endereços IPs, data e hora) e os dados de cadastro do usuário que realizou as conexões. Eventualmente o acesso à *Internet* do autor pode ocorrer de forma indireta, através de um serviço de tradução de endereços IPs e, nesse caso, serão necessários os registros de acesso do estabelecimento que forneceu esse serviço ao autor. No final do processo, os dados de cadastro do usuário ou os registros de acesso permitirão localizar o possível autor de um delito.

Sobre os registros de *logs*, de acordo com o Marco Civil da *Internet* [14], os provedores de conexão devem manter os registros de conexão por um prazo de 1 ano. Já os provedores de aplicações devem manter seus registros por um prazo de 6 meses.

Assim, se os IPs de onde foram originadas as ações investigadas forem identificados, será possível descobrir o local de onde a conexão foi realizada, sendo também possível indicar a autoria das ações.

III. METODOLOGIA

Inicialmente foi criado um ambiente controlado de testes para verificar os procedimentos, as técnicas e as ferramentas de análise de tráfego de redes necessários para identificar os endereços IPs. Em seguida, foi realizado um estudo de caso, no qual foi aplicado e verificado os resultados dos instrumentos e procedimentos descritos na fase de testes. Tanto na fase de testes como na de estudo de caso foram colhidos os dados de tráfegos de redes, os quais foram filtrados e analisados. Por fim, são apresentados os resultados dessas análises.

A. Instrumentos e procedimentos

O perito deve coletar e analisar um conjunto de vestígios relacionados ao caso investigado. No caso específico de

investigação em ambiente de jogos *online*, onde se busca a identificação do autor através do endereço de IP utilizado por ele, o método de trabalho, mostrado na Figura 5, é sugerido para a realização de coleta e análise de dados de tráfegos de rede.

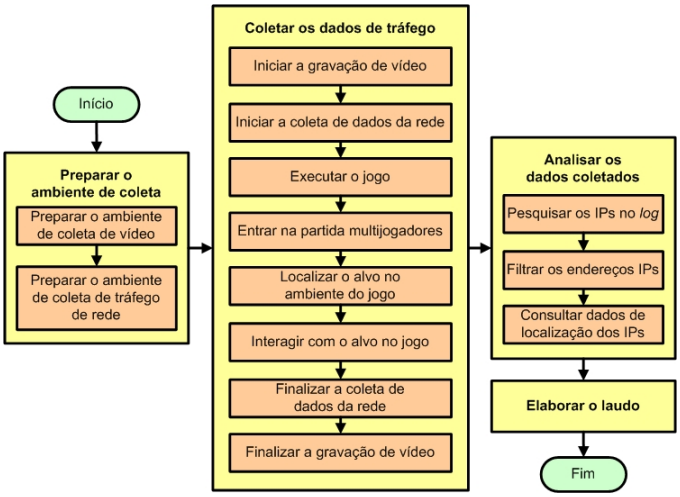

Fig. 5. Visão geral das fases de investigação e coleta de dados de tráfego de rede para jogos *online*.

O método apresentado consiste em 3 fases principais, quais sejam: (1) preparar o ambiente de coleta, (2) coletar os dados de tráfego, (3) analisar os dados coletados e (4) elaborar o laudo.

A fase de preparação do ambiente de coleta consiste na preparação do ambiente para coleta de dados de vídeo e dados de tráfego de redes. A coleta de vídeo é necessária para identificar os momentos do jogo nos quais ocorreram ou foram executados eventos de interesse pericial. Na Figura 6, são apresentados dois possíveis modelos de infraestrutura de equipamentos para realizar a coleta de dados de vídeo e rede, nos quais são utilizados uma câmera de vídeo, um monitor, um console de jogos, um computador coletor de dados da rede, um roteador e acesso à *Internet*.

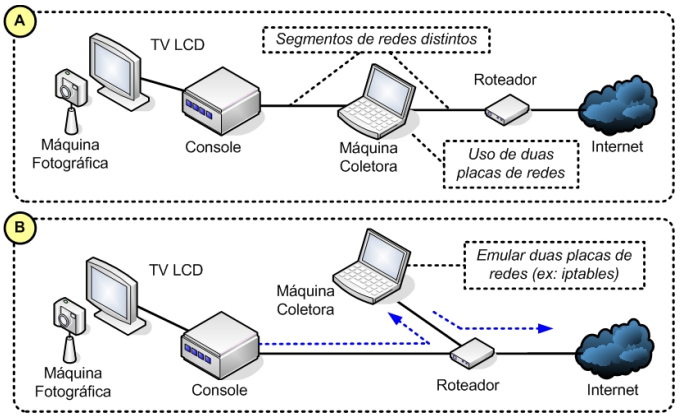

Fig. 6. Modelos de infraestrutura de equipamentos para a coleta de dados.

Na Figura 6-A, a máquina coletora possui duas placas de rede e fisicamente está *inline* no meio de acesso à *Internet*. Já na Figura 6-B, a máquina coletora emula duas placas de rede. Em ambos os casos, o console de jogos é configurado para utilizar a *interface* da máquina coletora como *default gateway*. Alternativamente, a máquina coletora pode ser configurada como ponte, conectando dois segmentos de redes distintos e operando em um nível mais baixo do modelo OSI (nível 2).

Na fase de coleta de dados de tráfego, deve-se iniciar a gravação da execução do jogo e a coleta dos dados de rede, os quais podem ser extraídos através do uso de *softwares* específicos como o *Wireshark* [12] e o *Tcpdump* [10]. Após a execução do jogo, deve-se localizar dentro do ambiente virtual do jogo o alvo. Nesse momento será necessária alguma interação com o alvo para que ocorra alguma troca de mensagens – e dessa forma ocorra a transmissão de pacotes IP.

Durante a fase de análise dos dados coletados, o perito deverá aplicar os filtros necessários para extrair os IPs possivelmente relacionados com o alvo. Pode-se proceder, então, a busca pela localização aproximada (e também as informações do provedor de conexão) de onde foi realizada a conexão que utilizou cada um dos IPs extraídos.

Por fim, os resultados dessas pesquisas deverão ser reportados no laudo pericial.

IV. ESTUDO DE CASO

O método descrito na *Seção III* foi aplicado na investigação de um caso real de furto em uma residência. Dentre os objetos furtados nessa residência havia um equipamento *Sony Playstation 3* (PS3) [15]. Dessa forma, foi percebido pela vítima que o criminoso (ou receptador) estava utilizando o perfil da vítima e jogando *online* o jogo *Call of Duty: Black Ops 2* [2] por meio do PS3 furtado, pois esse equipamento havia sido configurado para fazer o *login* automático na *PlayStation Network* (PSN) [16] com o perfil da vítima. Diante desse cenário, a autoridade policial solicitou a identificação do endereço IP de onde partiam os acessos do usuário da vítima para conectar na PSN.

A. Preparação do ambiente de coleta

Para a realização do exame é necessário que o console *Playstation 3* esteja conectado à *Internet*, para que ele possa acessar a PSN, e que os pacotes IP que chegam e saem do console sejam capturados, para análise posterior. Para isso, utilizou-se um computador entre o *Playstation 3* e a *Internet*, o qual realizava o roteamento dos pacotes e a sua captura. Assim, o modelo de infraestrutura utilizada foi o modelo ilustrado na Figura 6-B.

Buscando entender o funcionamento da PSN, foram realizados testes de diversas funcionalidades da rede do *Playstation 3*, tendo sido determinado que, para obter o endereço IP de um determinado jogador era necessário estar jogando o mesmo jogo e estar na mesma partida que ele.

Assim, através da conexão com a *Internet* é possível utilizar vários serviços da PSN. Há vários serviços de interação com outros usuários. Entretanto, a maioria das interações é intermediada pelos servidores da PSN, tais como *login*, *chat* e troca de mensagens. Entretanto, em jogos *online* de multijogadores, durante a interação direta entre os jogadores, ocorre a troca de mensagens entre esses jogadores, assim como entre os jogadores e o servidor da PSN. Nesse caso, como é mostrado na Figura 7, ocorre a troca de pacotes TCP e UDP com endereços IP específicos de cada usuário.

Dessa forma, durante o passo da coleta de dados da rede, os dados mais relevantes são aqueles coletados durante a interação com o alvo no ambiente virtual. Nesse sentido, a gravação em vídeo da execução da partida se torna relevante, já que através dela é possível identificar os momentos de interação com o alvo e, em seguida, filtrar os dados de tráfego relacionados a esse período.

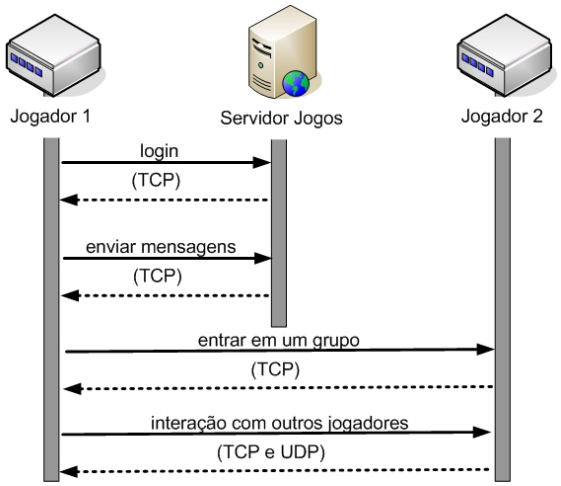

Fig. 7. Principais operações e protocolos utilizados durante a execução do jogo.

B. *Coleta dos dados de tráfego de rede*

O *software sniffer* instalado na máquina coletora foi o *tcpdump*. Através do comando `tcpdump -n` é possível iniciar a captura do tráfego. Assim, será mostrado todo o tráfego de rede, que passa pela primeira *interface* listada com o comando `tcpdump -D`, sem resolver nomes. Isso permitirá a visualização do tráfego em tempo real [7] [10].

Foram necessárias inúmeras tentativas para entrar na mesma partida ou jogo do alvo. Essa é a fase de formação dos grupos. Em geral, uma partida é iniciada com um grupo de 12 jogadores, divido em duas equipes rivais de 6 jogadores. Durante a partida alguns jogadores podem sair e outros jogadores podem entrar.

Na Figura 8, é apresentada a execução do jogo *Call of Duty: Black Ops 2*, no qual pode-se acessar quais são os nomes dos usuários que participam da partida. Na mesma figura é possível identificar os nomes utilizados pelo perito e pelo alvo dentro do ambiente do jogo.

Fig. 8. Imagem extraída do jogo *Call of Duty: Blacks Ops 2* [2].

A arquitetura frequentemente utilizada nos jogos multijogadores nos quais a posição de cada jogador é relevante é aquela baseada em mapas de 2 dimensões (2D). Tais mapas são divididos em quadrantes e quando ocorre a aproximação de jogadores no mesmo quadrante há a troca de pacotes TCP e UDP entre esses jogadores e a troca de pacotes TCP com o servidor de aplicação.

Na Figura 9, é mostrado graficamente um exemplo de uso de mapas 2D. Dessa forma, a fim de coletar os dados de tráfegos relevantes para a investigação, o perito deve "caçar" o alvo dentro do ambiente virtual.

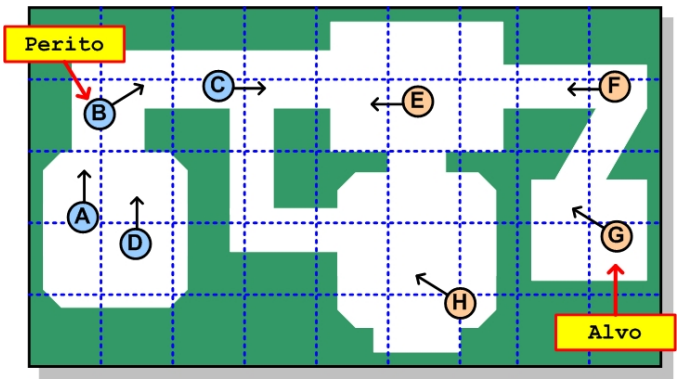

Fig. 9. Modelo de mapa 2D utilizado pelo jogo.
Fonte: Adaptado de Brackeen et al. [1].

Assim, foram feitas diversas tentativas para entrar no mesmo jogo e interagir com o alvo. As tentativas foram feitas em dias e horários diferentes. Durante essas tentativas foram capturados os pacotes IP que trafegavam entre o PS3 e a *Internet*, bem como foram tiradas fotos dos jogadores e gravados vídeos do jogo no ambiente virtual. Como resultado, foram coletados 3 arquivos de captura de tráfego de 3 jogos distintos nos quais o alvo esteve presente.

C. *Análise dos dados coletados*

Os pacotes IP de cada jogo foram filtrados, eliminando-se os IPs dos servidores da empresa *Sony* e pacotes não relacionados ao jogo (tais como pacotes de consultas DNS). A análise dos dados coletados foi realizada no ambiente *GNU Linux*, por meio de um interpretador de comandos *Shell* [18].

Os comandos destacados no Quadro 1 foram utilizados para realizar a extração ordenada dos endereços IPs, através do comando `egrep`, que pesquisa e apresenta os somente as partes do arquivo que possuem o padrão da entrada, e do comando `sort`, que ordena o resultado.

QUADRO 1. COMANDOS DE FILTRAGEM DE ENDEREÇOS IPS.

```
cat captura-jogo3.txt
↳ | egrep -o '[0-9]{1,3}\.[0-9]{1,3}\.
↳ [0-9]{1,3}\.[0-9]{1,3}'
↳ | sort > lista-ips-jogo.txt
> 177.17.138.229
> 177.17.138.229
> ...
> 177.193.12.107
> 177.193.12.107
> ...
> 177.41.254.5
> 177.41.254.5
> ...
```

Em seguida, foram extraídos os IPs do servidor de jogos da PSN, assim como os endereços da rede local (ver Quadro 2).

QUADRO 2. LISTA DE IPS DE REDE LOCAL.

```
>    10.0.0.0 -  10.255.255.255(10/8 prefix)
>  172.16.0.0 -  172.31.255.255(172.16/12 prefix)
> 192.168.0.0 - 192.168.255.255(192.168/16 prefix)
```

Sobre a lista de IPs resultantes, foram contadas o número de ocorrências de cada IP, como apresenta o Quadro 3. Nesse quadro, o comando `uniq -c` é usado para contar o número de repetições da entrada ordenada, e o comando `sort -r` ordena o resultado em ordem reversa. O resultado é apresentado em

duas colunas, que são o número de ocorrências e o endereço IP relacionado.

QUADRO 3. COMANDOS DE CONTAGEM DE FREQUÊNCIA DOS ENDEREÇOS IP.

```
cat lista-ips-jogo3.txt | uniq -c
↳ | sort -r > lista-ips-count-rev.txt
> 3385 177.80.118.68
> 2630 201.52.52.162
> 2540 200.206.146.200
> 1835 186.220.199.241
> 1830 177.193.12.107
> 1715 187.39.163.177
> 1255 189.102.126.154
>  905 189.123.225.196
>  220 187.39.71.57
>  154 201.92.213.21
>  120 179.197.122.237
>  100 189.120.250.17
>   55 177.41.254.5
>   55 177.17.138.229
>   45 190.176.222.87
```

Após essa filtragem, os endereços IP restantes possuíam quantidade compatível com o número de jogadores presentes em cada jogo. Deve-se ressaltar que, em alguns jogos, a quantidade de IPs ultrapassa o número máximo de jogadores em cada partida (12 jogadores) devido ao fato de, durante o jogo, alguns jogadores deixarem a partida e outros entrarem em seus lugares.

Em seguida, foi realizado um cruzamento de dados para verificar qual IP ou qual par provedor/cidade se mantinha constante nos três jogos. Foi necessário analisar o par provedor/cidade, e não somente o IP, pois, como a maioria dos acessos domésticos à *Internet* utilizam alocação dinâmica de IP, é possível que o IP de um determinado jogador tenha sido trocado entre os três jogos analisados, principalmente nos que ocorreram em dias distintos.

Uma das consultas de localização foi através do `geoiplookup`, utilizando os comandos do Quadro 4, cujo resultado da execução dos comandos são duas colunas com o endereço IP e os dados de localização.

QUADRO 4. COMANDOS DE CONSULTAS DE LOCALIZAÇÃO DE ENDEREÇOS IPS.

```
for i in $(cat lista-ips-uniq.txt);
   do r=$(geoiplookup $i);
   echo $i - $r;
done
> 177.17.138.229  - GeoIP: BR, Brazil
> 177.193.12.107  - GeoIP: IP Address not found
> 177.41.254.5    - GeoIP: BR, Brazil
> 177.80.118.68   - GeoIP: BR, Brazil
> 186.220.199.241 - GeoIP: BR, Brazil
> 187.39.163.177  - GeoIP: BR, Brazil
> 187.39.71.57    - GeoIP: BR, Brazil
> 189.1.174.20    - GeoIP: BR, Brazil
> 189.102.126.154 - GeoIP: BR, Brazil
> 189.120.250.17  - GeoIP: BR, Brazil
> 189.123.225.196 - GeoIP: BR, Brazil
> 190.176.222.87  - GeoIP: AR, Argentina
> 200.206.146.200 - GeoIP: BR, Brazil
> 201.52.52.162   - GeoIP: BR, Brazil
> 201.92.213.21   - GeoIP: BR, Brazil
```

Além da consulta de localização do `geoiplookup` outras ferramentas para levantamento de dados podem ser utilizadas: `geoip`, `nslookup`, `wget` e `whois`. O Quadro 5 apresenta um exemplo de resultado da consulta `whois`.

QUADRO 5. RESULTADO DA CONSULTA DO COMANDO WHOIS.

```
whois 177.193.12.107
> ...
> inetnum:      177.192/14
> aut-num:      AS28573
> abuse-c:      GRSVI
> owner:        NET Servicos de Comunicacao S.A.
> ownerid:      000.108.786/0001-65
> responsible:  Grupo de Seguranca da Informacao Virtua
> country:      BR
> owner-c:      GRSVI
> tech-c:       GRSVI
>...
```

A Tabela 2 mostra o resultado consolidado das coletas realizadas em 3 jogos distintos (nos quais houve a participação do usuário alvo), com os dados de IP, de localização e do provedor de conexão.

TABELA II. RESULTADO DA ANÁLISE DOS IPS COLETADOS

Jogo 1	Jogo 2	Jogo 3	Provedor/Cidade
	54.9.9.4		Woodbridge – NJ - USA
177.133.29.165	**177.133.29.165**		**GVT - Sobradinho - DF**
177.143.201.90			Virtua - Farroupilha - RS
177.4.237.10			**Brasil Telecom S/A - Filial DF**
		177.17.138.229	**GVT Brasília – DF**
	177.32.41.148		Virtua - Sao Paulo - SP
		177.41.254.5	GVT - Joinville - SC
177.42.208.116			GVT - Salvador - BA
		177.80.118.68	Virtua - Sao Paulo - SP
177.96.164.233			GVT - Palhoça - SC
177.96.177.158			GVT - Curitiba - PR
177.96.38.186			GVT - Palhoça - SC
177.100.114.223			VCB - Macaé - RJ
177.106.213.223			CTBC - Uberlândia - MG
177.106.245.43			CTBC - Uberlândia - MG
	177.141.117.100		Virtua - São Paulo - SP
	177.179.234.217		Oi Velox - Rio de Janeiro - RJ
		177.193.12.107	Virtua - São Luís - MA
		179.197.122.237	Oi Velox - Brasil
		186.220.199.241	Virtua - Sao Paulo - SP
	187.35.24.94		Vivo - São Paulo - SP
		187.39.71.57	Virtua - Pindamonhangaba - SP
		187.39.163.177	Virtua - Bento Gonçalves - RS
187.112.240.107			GVT - Cascavel - PR
		189.1.174.20	Hostlocation - São Paulo - SP
	189.6.13.13		Virtua - Brasil
	189.27.84.106		GVT - Campo Grande - MS
189.73.249.39			BR Telecom DF - MS
189.81.47.23			Velox - João Pessoa - PB
189.85.178.19			Newsite - Palhoça - SC
	189.102.45.194		Virtua - São Paulo - SP
		189.102.126.154	Virtua - São Paulo - SP
		189.120.250.17	Virtua - São Paulo - SP
		189.123.225.196	Virtua - Curitiba - PR
		190.176.222.87	Telefonica – Argentina
200.193.245.146			**BR Telecom DF - Brasilia - DF**
		200.206.146.200	Vivo - Indaiatuba - SP
	201.22.89.163		GVT - Maringá - PR
		201.52.52.162	Virtua - Sao Paulo - SP
	201.74.34.15		Virtua - São Bernardo - SP
201.86.0.95			GVT - Curitiba - PR
		201.92.213.21	Vivo - Santana de Parnaíba - SP

São destacados na Tabela II, em negrito, os endereços IPs sediados no Distrito Federal. O IP `177.133.29.165` foi o

único a se manter nos jogos 1 e 2 e o IP 177.17.138.229 foi o único do Distrito Federal no jogo 3. Ademais, ambos IPs são da empresa GVT, sendo, portanto, os IPs mais prováveis de estarem vinculados ao usuário alvo.

Foi realizado, também, o cruzamento dos nomes dos jogadores capturados por fotografias durante as partidas. Ressalta-se que as fotografias mostram os jogadores presentes no jogo em determinado momento, pois ocorrem algumas trocas de jogadores durante o jogo.

Assim, foi preparado o laudo para a autoridade policial, relatando o método de trabalho, assim como os resultados obtidos. Esses resultados incluem um conjunto de registros contendo os dados de IP, provedor, cidade, data e hora. Esses dados são suficientes para buscar, por meio do provedor de conexão, o usuário que utilizou tais IPs nos períodos especificados.

V. Conclusões

Os ambientes virtuais criados na *Internet,* tais como os jogos *online* multijogadores são cada vez mais utilizados para cometer crimes. Por meio de uma metodologia de investigação baseada na análise de tráfego de redes é possível coletar mensagens de protocolos de rede como o TCP, UDP e IP para auxiliar no estabelecimento da autoria de um crime, até mesmo de crimes iniciados fora desse ambiente, como um furto.

Para isso, é necessário entender o contexto dos jogos *online*. Dessa forma, foi apresentado o modelo lógico da arquitetura de um sistema de jogo, tendo como principais camadas a aplicação, lógica, visão do jogo e visão remota. Também é necessário entender as várias formas de interação entre os jogadores e o sistema de jogo (*single player*, *multiplayer*, etc.).

A metodologia proposta neste trabalho é adequada para os modelos de arquitetura de jogos do tipo *multiplayer*, ou seja, para aqueles jogos que envolvem 2 ou mais jogadores interagindo entre si através de uma conexão de *Internet* e, ainda, sabendo-se o nome virtual do alvo e interagindo com ele. Ela inclui a preparação do ambiente, a coleta de dados de tráfego de redes, a análise dos dados coletados e a apresentação do laudo.

A aplicação da metodologia em um caso real demonstrou a viabilidade de coletar dados de vídeo e rede em serviços de jogos *online*. Também revelou a importância das informações de vídeo para identificar os eventos de interesse pericial, nos quais ocorreram a interação com o alvo, os quais, após um processo de análise e filtragem, permitiram identificar os IPs relacionados ao alvo da investigação.

Esses endereços IP (em data e hora delimitados) são essenciais para o prosseguimento da investigação, que passará a depender de dados fornecidos pelo provedor de aplicação, provedor de conexão e, em alguns casos, de estabelecimento público ou privado. Sem eles, não é possível descobrir o local de onde a conexão foi realizada e, consequentemente, estabelecer a autoria das ações.

A aplicação da metodologia em outras plataformas e serviços de jogos *online* é uma das possibilidades de trabalhos futuros. Outra possibilidade é a avaliação do impacto da utilização de servidores *proxy* (e outras técnicas de camuflagem) na metodologia proposta, especialmente na coleta de vestígios.

Referências

[1] Brackeen, David; Barker, Bret; Vanhelsuwé, Laurence. “Developing Games in Java”. New Riders, 2003.

[2] *Call of Duty* disponível em http://www.callofduty.com/, acessado em 30/05/2015.

[3] Cardoso, Nágila Magalhães; Hashimoto, Yuri Campos; da Silva, Keith Maila Domingos; Maia, Anderson Trindade. “Redes sociais a nova arma do crime cibernético: O efeito do uso da engenharia social e da esteganografia”. The International Journal of Forensic Computer Science (ICoFCS), 2011.

[4] CGI, disponível em http://cgi.br/, acessado em 30/05/2015.

[5] Fullerton, Tracy. “Game Design Workshop: A Playcentric Approach to Creating Innovative Games”. A K Peters/CRC Press, 2014.

[6] Mcshaffry, Mike; Graham, David. “Game Coding Complete”. Course Technology PTR, 2012.

[7] Mota Filho, João Eriberto. “Análise de Tráfego em Redes TCP/IP: utilize tcpdump na análise de tráfego em qualquer sistema operacional”. Novatec Editora, 2013.

[8] Peron, André; de Deus, Flávio Elias Gomes; de Sousa Júnior, Rafael Timóteo. “Ferramentas e Metodologia para Simplificar Investigações Criminais Utilizando Interceptação Telemática”. The International Journal of Forensic Computer Science (ICoFCS), 2011.

[9] Rabin, Steve. “Introduction to Game Development”. Course Technology PTR, 2009.

[10] Tcpdump, disponível em http://www.tcpdump.org/, acessado em 30/05/2015.

[11] Vecchia, Evandro Della. “Perícia Digital: da investigação a análise forense”. Millenium Editora, 2014.

[12] Zimmermann, Hubert. "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection". IEEE Transactions on Communications, 1980.

[13] Wireshark, disponível em http://www.wireshark.org/, acessado em 30/05/2015.

[14] Brasil. Lei no 12.965, de 23 de abril de 2014.

[15] *Sony Playstation 3*, disponível em http://br.playstation.com/ps3/, acessado em 30/05/2015.

[16] *PlayStation Network*, disponível em http://br.playstation.com/psn/, acessado em 30/05/2015.

[17] *Internet Assigned Numbers Authority*, disponível em http://www.iana.org, acessado em 30/05/2015.

[18] Neves, Julio Cezar. “Programação Shell Linux”. Editora Brasport, 2010.

Juliano K. M. Oya e Cleber Scolarick Junior, Peritos Criminais, Seção de Perícias em Informática, Instituto de Criminalística – Polícia Civil do Distrito Federal, Brasília-DF, Brasil. E-mails: juliano.oya@gmail.com e scoralick@gmail.com

Bruno W. P. Hoelz, Perito Criminal, Instituto Nacional de Criminalística – Polícia Federal, Brasília-DF, Brasil. E-mail: werneck.bwph@pdf.gov.br