SEOULTECH

SeoulTech UCS Lab
Ubiquitous Computing & Security Laboratory

A cloud-based forensics tracking scheme for online social network clients

Presented by
Nam Yong Kim
(nykim@seoultech.ac.kr)

Abstract

- In recent years, with significant changes in the communication modes, most users are diverted to cloud-based applications, especially online social networks (OSNs), which applications are mostly hosted on the outside and available to criminals, enabling them to impede criminal investigations and intelligence gathering.

- In the virtual world, how the Law Enforcement Agency (LEA) identifies the ‘‘actual’’ identity of criminal suspects, and their geolocation in social networks, is a major challenge to current digital investigation.

- this paper proposes a scheme, based on the concepts of IP location and network forensics, which aims to develop forensics tracking on OSNs.

- To the best of our knowledge, this is the first individualized location method and architecture developed and evaluated in OSNs.

1. Introduction

- In recent years, with significant changes in communication modes, most users are diverted to cloud-based applications, especially online social networks (OSNs), such as Facebook and Twitter.

- Individuals can access social network messaging communications and remain within Facebook or other social networks, and through chat windows, can write on someone else's wall or their own wall, and as social network data center/servers may be in another country, unlike call detail records, metadata are not available and contents are encrypted.

- Despite being primarily used to communicate and socialize with friends, the diverse and anonymous nature of social networking websites makes them highly vulnerable to cybercrimes. Phishers, fraudsters, child predators, and other cyber criminals, can register at these services with fake identities, hiding their malicious intentions behind innocent appearing profiles.

1. Introduction

- The large number of criminal acts that can be performed through social networks raises the importance of identifying the ‘‘actual’’ identity and location of cyber-criminal suspects in the digital virtual world.

- However, the aforesaid topic, to the best of our knowledge, has not been thoroughly studied. Related research on how to gather digital evidence of OSNs mainly uses traditional digital forensics for acquisition of smartphones, and is focused on acquisition techniques and general forensic analysis.

- They believe that potential evidence can be held on user devices and recovered with the right tools and examination methods. The data that could be extracted from the internal memory of these devices include call logs, SMS, MMS, emails, webpage bookmarks, photos, videos, and calendar notes.

- Recent scientific research has focuses on individual types of smartphones, and investigation methods that could be used to acquire and analyze data, through either physical or logical methods.

1. Introduction

- The above mentioned data sources were organized in a taxonomy of evidence types: identity evidence, location evidence, time evidence, context evidence, motivation evidence, and means evidence, which are derived from a set of questions i.e: who, where, when, what, why, and how.

- However, the application of this method is limited to searching the mobile phones of target clients. Unfortunately, this assumption is inappropriate for many real-world applications.

- The related research indicated that traditional approaches to forensics on cloud computing and social network forensics are insufficient from organizational and technical perspectives, while traditional digital forensics is based on the analysis of file systems and captured network traffic.

1. Introduction

To individually analyze a targeted service resource identifier (SRI) and locate its location in online social network applications, there are some challenges that still require solutions, as follows.

1. multiple cyber-identities and applications.

2. the majority of social network services switch rapidly over to hypertext transfer protocol secure (HTTPS) versions, and there is a growing range of sophisticated, encrypted communication channels to exploit.

3. relevant information is obtained only from the payload of the application layer, is spread over multiple packets/sessions, and must be highly correlated, in order to obtain the metadata related to SRI location measurement (i.e. application layer location measurement) and individualized analysis.

4. IP location issue.

1. Introduction

- This is a difficult problem, even putting mobility aside, as the decentralized management of the Internet means that there is no authoritative database of host locations. The databases that do exist are derived by combining a mix of sources (including domain name system (DNS) type mnemonic records, who the site is registered to, and DNS hostname parsing rules), which are all manually maintained, and thus, subject to inconsistencies and outdated information.

- The ‘‘CloudTracker’’ mechanism, as proposed in this study, is based on the concepts of IP Location and Network Forensics, which develops forensics tracking aims to instantly trace the ‘‘physical location’’ of targeted SRI, when the target client is using online social network applications, and associatively analyze probable ‘‘identity’’.

2. Related Works

2.1. Mobile device forensics

- Smartphones constantly interweave into everyday life, as they accompany individuals in different contexts. It is believed that smartphones include a combination of heterogeneous data sources, which can prove essential when combating crime.

- Forensic examination of smartphones is challenging, as they are always active and are constantly updating data, which can cause faster loss of evidentiary data.

- Second, the operating systems (OS) of smartphones are generally closed sources, with the notable exception of Linux-based smartphones, which makes creating custom tools to retrieve evidence a difficult task for forensic examiners. In addition, smartphone vendors tend to release OS updates very often, making it hard for forensic examiners to keep up with the examination methods and tools required to forensically examine each release. The variety of proprietary hardware of smartphones is another issue faced by forensic examiners.

2. Related Works

- From the initial works of the mobile device forensics field, later research provided foundational concepts on forensic analyses of new generations of smartphones(e.g.BlackBerry and iPhone), to recent scientific research focused on individual types of smartphones and investigating methods, there has been complete review in Mutawa et al's work.
- They further focus on conducting forensic analyses on three widely used social networking applications of smartphones: Facebook, Twitter, and MySpace which were aimed at determining whether activities conducted through these applications were stored on the device's internal memory.
- Mylonas et al proposed a proactive smartphone investigation scheme that focuses on ad-hoc acquisition of smartphone evidence. They also consider the legal implications of the proposed scheme.
- Lee and Hong introduced a service concept called ''forensic cloud'' to develop new paradigms in digital forensics. Furthermore, in order to show the feasibility of the concept, the paper suggested a technology framework for forensic analysis, as based on the mobile cloud, in order to describe the current status of its development.
- However, previous approaches suffered from the problem of assuming the availability of the target client's smartphone. The forensic tracking mechanism, as discussed in his paper, is underpinned by Network Forensics rather than by Mobile Device Forensics.

2. Related Works

2.2. Man-in-the-middle attack

- There are two general approaches to meet HTTPS protocol challenges.
  1. First, in some cases, we can capture traffic and use the server's private key to recover the session keys and decrypt the contents (depending on the method of key exchange), which requires that we have access to server's private key either before or after the traffic capture.
  2. Second, we can intercept the transport layer security/secure sockets layer (TLS/SSL) session using a manin-the-middle (MITM) proxy.

- As most well-known applications (services) are foreign venders, the practitioners are unwilling to provide private keys without jurisdiction. therefore, Law Enforcement Agency (LEA) only adopts approach number two to solve the problem of HTTPS encrypted communication protocol.

- Web-based applications rely on the HTTPS protocol to guarantee privacy and security. Users trust this protocol to prevent unauthorized viewing of their personal and confidential information over the web.

2. Related Works

- The MITM attack exploits the fact that the HTTPS server sends a certificate with its public key to the web browser.

- If this certificate is not trustworthy, the entire communication path is vulnerable. Such an attack replaces the original certificate authenticating the HTTPS server with a modified certificate. The attack is successful if the user neglects to double-check the certificate when the browser sends a warning notification.

- Research activities already have various works to deal with HTTPS.

- Burkholder analyzed the SSL handshake defect and verified the possibility of attack to SSL. Callegati et al described conducting SSL attacks by webmitm.

- However, previous research has been limited to the LAN environment. The MITM proxy, as proposed by this study, is designed with reference to the Suga's model, to proposes an Inline Redirection model, which attempts to be implemented in large-scale third generation (3G) universal mobile telecommunications system (UMTS) networks.

3. System architecture and the main elements

3.1. System architecture

The system architecture of our CloudTracker is as depicted in Fig. 1, including four subsystems,

1. MITM proxy
2. Data Retention System
3. Location Information Retrieval Agent
4. Location Calculation Engine

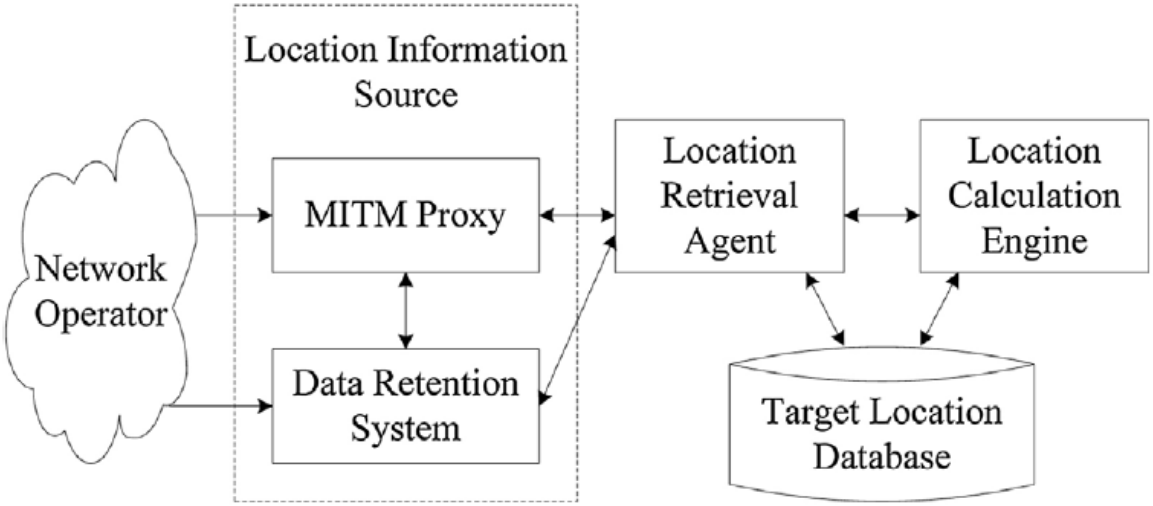

Fig. 1. The CloudTracker framework.

3. System architecture and the main elements

3.2. MITM proxy

The MITM proxy subsystem in the CloudTracker framework is built into the Internet service provider (ISP) network with the assistance of domestic ISP practitioners in order to capture and inspect the contents of TLS/SSL-encrypted traffic, and change the original encrypted channel between client and online social network servers into two encrypted channels, as shown in Fig. 2.

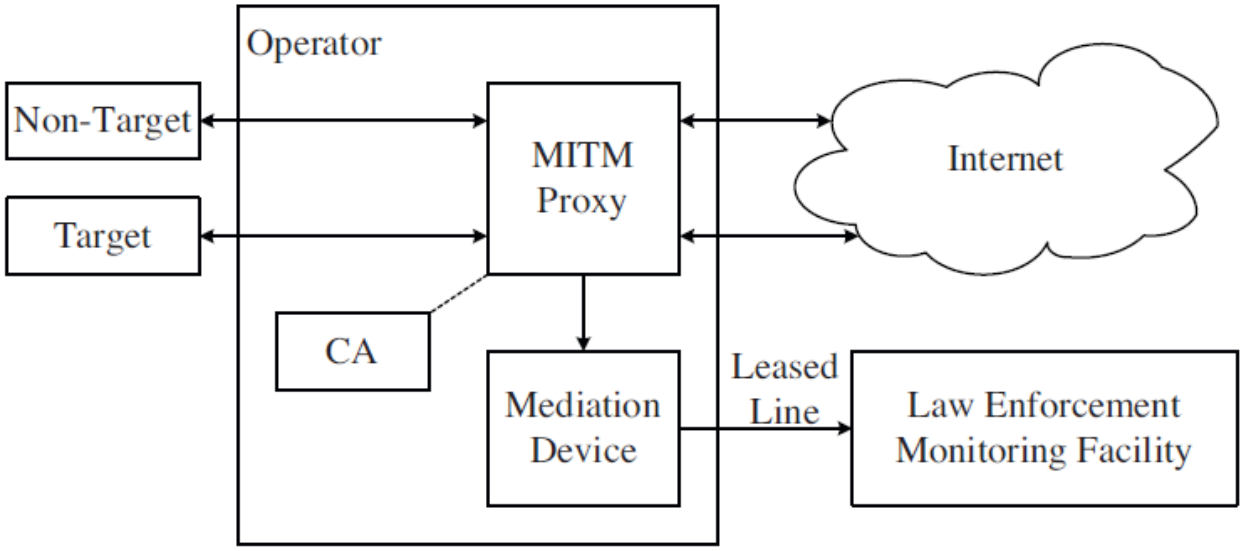

Fig. 2. MITM proxy defeat HTTPS Model.

3. System architecture and the main elements

One is the MITM proxy client, the other is the MITM proxy server. Thus, the MITM Proxy can see bidirectional clear data between client and server, as shown in Fig. 3.

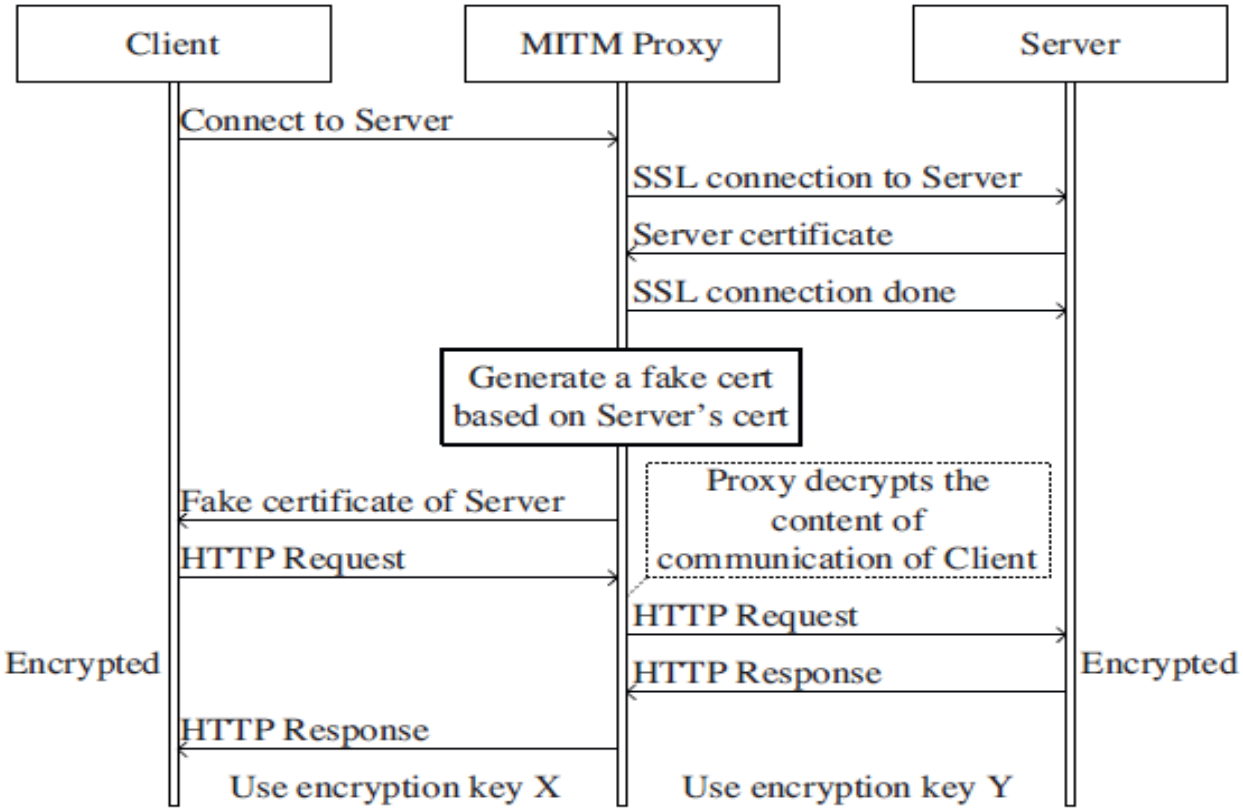

Fig. 3. HTTPS MITM (TLS/SSL proxy).

3. System architecture and the main elements

3.3. Data retention system

In a general way, the authentication of logins is divided into one-stage authentication (united Internet Access and Application Services) and two-stage authentication (respective authentication of Internet Access and Application Services).

The packets of authentication contain;

(1) Numbers to ID physical devices (IMEI, MAC, etc.).

(2) Numbers to ID logical or physical endpoints (IP,E.164, etc.).

(3) Service resource identifiers (E-mail-address, TELURI, SIP-URI, etc.) location information. The information of these logins will be the basis of Application Layer Location Measurement (i.e. SRI Location Measurement) and Individualization Analysis.

in most cases, using passive probes is the only way to obtain outside hosted application service activity data.

3. System architecture and the main elements

In view of this, this study attempts to lay intelligent probe sensors (IPS) with deep packet inspection (DPI) functions in front of or behind the (soft) switch of the Access Network, for example, between SGSN (serving GPRS(General Packet Radio Service) support node) and GGSN (gateway GPRS support node) of 3G UMTS(Universal Mobile Telecommunication System) networks for generations of application-level logs.

In a passively monitored network, the information of the Application Layer Location Measurement can be obtained in the course of application services authentication, and the ‘‘call logs’’ of Internet based communications can be generated; including activity events and IP data retentions (IPDRs), which can be the base of communication relation network analysis.

On the other hand, the information of the Network Layer Location Measurement (i.e. IP location) can be obtained in the course of Internet access authentication. This subsystem stores the important information of SRI intercepted by IPS (e.g. Facebook, Twitter, etc.), login time, and IP.

This paper analyzes different Access Networks (xDSL, 3G UMTS, WiFi, and LTE), and utilizes different OSNs applications, in order to implement data retention system for the following information as the key information of SRI Location Measurement and Individualization Analysis:

3. System architecture and the main elements

3.3.1. Internet access (DHCP, RADIUS) information

(1) use access network ID to inquire Internet connection logs.

(2) use IP + time range to trace back to access network ID. To save corresponding Access Network ID, IP, and timestamps. Access Network ID contains MSISDN, MAC, RADIUS account, circuit ID, etc. (the aforesaid information is classified as Access Information).

3.3.2. Private IP/public IP mapping (NAT/PAT mapping)

(1) sometimes only the public IP of an enterprise extranet is traced, and the private IP inside the enterprise cannot be traced, thus, the specific target cannot be individualized.

(2) the external (public IP: port, timestamp) is given, and the internal (Private IP: Port) is searched. To save enterprises, Internet cafes, small ISP Intranet private IP: port, converted by NAT/PAT into extranet public IP: port (the aforesaid information is classified as Access Information).

3. System architecture and the main elements

3.3.3. IP 5-tuple

(1) check whether there is a connection between a source IP and destination IP, i.e. decide which OSN applications to use.

(2) IP - [DNS Lookup] - Domain Name;

(3) IP/Domain Name - [Whois] - Detail Registration Information. To save all source IP, source Port, destination IP, destination Port, TCP/UDP, and timestamp (the aforesaid information is classified as Service Information).

3.3.4. Internet application login information

(1) according to the given Facebook Account of a suspect, which IP: Port they used and when they logged in can be searched.

(2) analyze the suspect's habit of using Facebook.

To save the user login information of popular Internet applications, including account, IP: port, timestamp, e.g. Facebook, Twitter, Plurk, etc. (the aforesaid information is classified as Service Information).

3. System architecture and the main elements

3.3.5. Provision data

The provision data, as administered by a network administrator, are integrated into the key information of SRI Location Measurement (see Table 1), including Service Information), Access Information, and Termination Information.

Table 1
Information for application layer location measurement.

	Termination information	Access information	Service information
Definition	The information that identifies a particular terminal is called terminal information	The information related to how the terminal accesses the Internet is called access information	Data of application services logins and IP call data record
Variability	Data seldom change	Data often change, especially in the environment of dynamic acquisition of IP	Data often change
Acquisition mode	Provided by network administrator, also known as provisioning data	Obtained from the existing network communication equipment or communication protocols	Obtained from metadata of application layer

3. System architecture and the main elements

3.4. Location information retrieval agent

The location information retrieval agent is in charge.

(1) mastering how to logically obtain a location from target identification data. For example, how to obtain location information when only the Facebook Account is known.

(2) gathering location information of target, and storing it in target location database.

3.5. Location calculation engine (profiler)

Location calculation engine (profiler) provides various geo information analysis functions, e.g. SRI Location Measurement (see Section 4.1) and target client trace reconstruction (see Section 4.2).

3.6. Legal issues

The Location retrieval Agent is also responsible for managing how, when, and to whom location is given. This is the way the privacy of the Target is protected in the CloudTracker mechanism. The Location retrieval Agent follows a set of rules called authorization policy, when making decisions about whether or not it should give location information to a particular Location Recipient. In practical, it is warrant requirement.

4. Forensics tracking analysis

4.1. SRI location measurements

A Location Measurement is a datum that can be used to locate a target/device (An online social network client). The Location Calculation Engine uses measurements to determine location, and a location measurement can be used as a key into a Target Location Database. Location measurement also can be thought of as a series of clues (i.e. Service Information, Access Information, Termination Information) that can be matched to some specific data (ex. IP, IMSI/IMEI/MSISDN) to form a chain (see Fig. 4).

At the start of this chain is a Application Layer ID (Facebook Account, Twitter Account, etc.), and at the other end is a Real ID (Name, ID, Location). SRI Location Measurements form some of the links of this chain in Target Location Database in the CloudTracker framework.

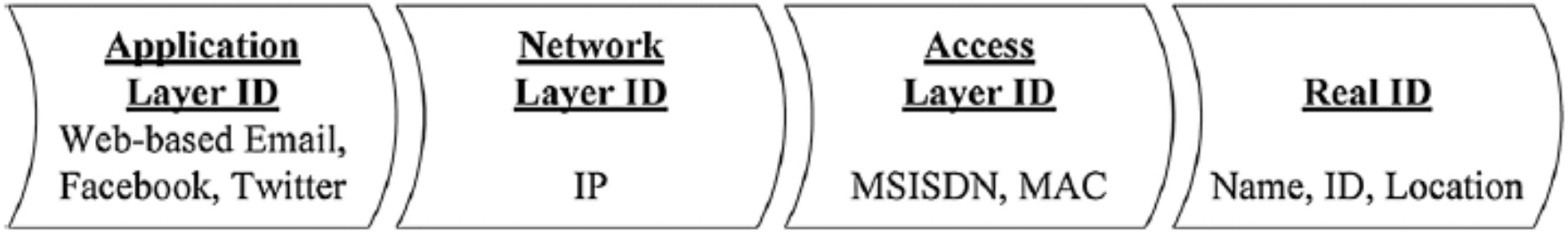

Fig. 4. Correlation information chains for SRI location measurement.

4. Forensics tracking analysis

Fig. 5 shows how this chain is formed for a 3G UMTS network. The area of uncertainty of SRI location measurement depends on different access networks. If the Target clients access the Internet via a fixed network, e.g. xDSL, the SRI Location Measurement can directly locate the actual position of the end IP device.

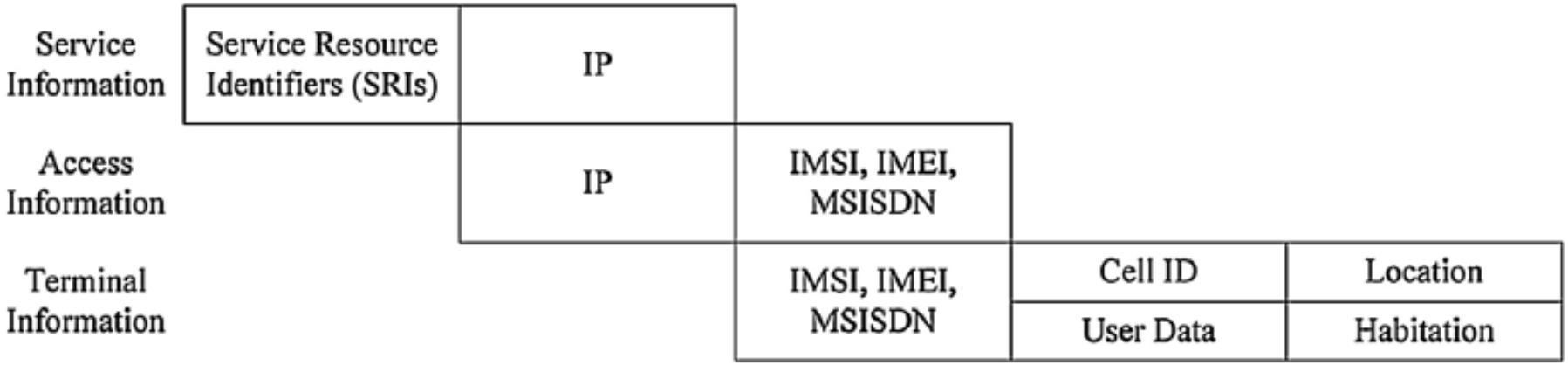

Fig. 5. Correlation information chains of 3G UMTS network.

4. Forensics tracking analysis

If they access the Internet via a mobile network (3/3.5G), the base station coverage (cell) can be located. The uncertainty range depends on the planned coverage of the base station.

For example, the radius is 150–500 m in urban areas, and 1–5 km in the suburbs. The ‘‘accuracy rate’’ is used to evaluate the percentage of correct location measurement. Its equation is defined as follows.

$$\text{Accuracy rate} = \frac{(\text{total number of Location Measurement} - \text{number of wrong Location Measurement}) \times 100\ (\%)}{\text{total number of Location Measurement}}$$

The right Location Measurement meaning a given Service Information (SRI) can be correlated with Access information and Terminal Information to link SRI to Location (the actual position of the end IP device if the Target clients access Internet via a fixed network, e.g. xDSL, or the base station coverage via a mobile network (3/3.5G)) and Target Client (User Data) (see Fig. 5). The SRI Location Measurement result of the proposed CloudTracker mechanism is measured by the ‘‘accuracy rate’’ index.

4. Forensics tracking analysis

4.2. Trace reconstruction

After SRI Location Measurement and Individualization Analysis, the ISP provider that issued the IP can be known. If it is from a fixed network, there is no trace reconstruction. If it is from a mobile network, the historical track of the online social network target client (e.g. track formed of cells) can be reconstructed, as based on user data obtained by individualization analysis, as well as the historical call data record(CDR) of the billing system of the ISP provider.

4. Forensics tracking analysis

4.3. Real world applications

The proposed CloudTracker mechanism is based on the concepts of IP Location and Network Forensics, meaning that, in an environment of an integrated fixed network, mobile telecommunication network 3/3.5G, and next generation network IP multimedia subsystem (IMS), each related node in the network is confirmed, the MITM proxy in charge defeats HTTPS, and the IPS (with deep packet inspection (DPI) functions) is in charge of accessing, copying, decoding, and saving necessary data retention for Application Layer Location Measurement (SRI Location Measurement).

Based on this mechanism, users can analyze the location of the SRI and associatively identify target client users according to a given SRI and time. Which implies that, implementing the proposed Cloud-Tracker mechanism on related nodes of various access networks and collecting the related information (i.e. Service Information, Access Information, Termination Information), can be beneficial for future cybercrime investigation.

When LEA is trying to locate a suspicious account, a Facebook account for example, the location of the suspicious application service account can be located by the search interface of CloudTracker (a location or coverage range of a base station that serves the target for browsing the Internet), and lead to identify the user of the suspicious account by associated analysis.

5. Empirical evaluation and discussion

5.1. Test environment and requirements

Prior to conducting the experiment, a forensics framework was set up and configured. This study implemented the proposed CloudTracker mechanism in a 3/3.5G UMTS network for evaluation,as shown in Fig. 6.

The red circles are the core components of the CloudTracker mechanism-IPS (Tap, Probe, DPI server) and MITM proxy.). The major function of the network tap is to completely copy the packets transmitted in the network. It is required to reduce the effect on the transmission line quality and rate as much as possible during copying.

In this experimental environment, the network tap is installed between SGSN and GGSN, and aimed to intercept the GPRS tunneling protocol (GTP) communication protocol. The intercepted GTP packet is led in the DPI server for deep decoding.

The Probe is in charge of filtering the communication content of the target client (network packet), identified as the IP (not MSISDN).

The communication content can be divided into identifiable encrypted communication, e.g. port 443, specific websites (e.g. Facebook, Twitter, etc.). These encrypted communications can be decrypted by MITM. The Probe leads the ‘‘identifiable encrypted communication’’ packet to the MITM server, while the other packets are copied and transmitted to mediation device (MD).

5. Empirical evaluation and discussion

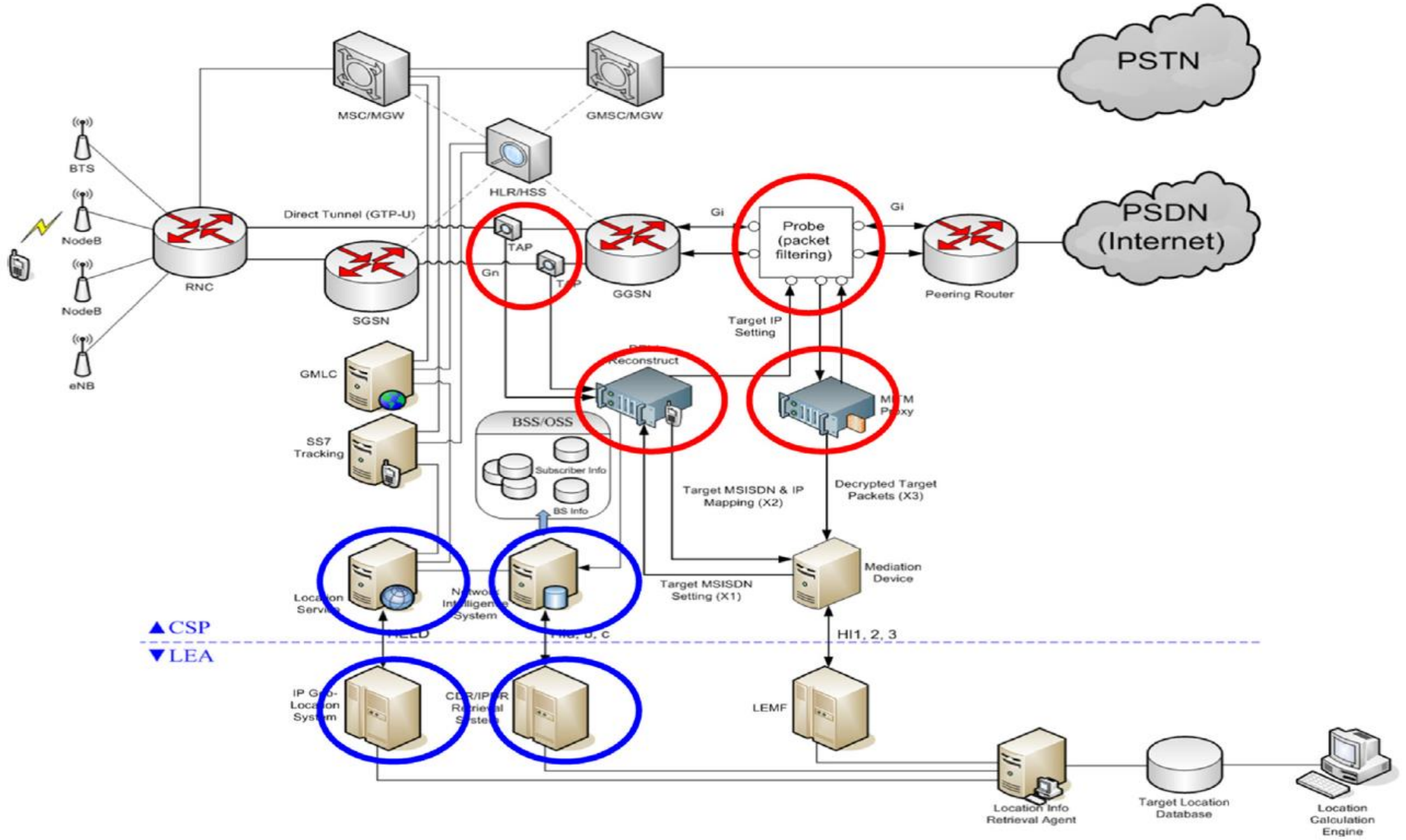

Fig. 6. Implementation of CloudTracker mechanism in 3/3.5G network. (Inline Redirection model)

5. Empirical evaluation and discussion

All network packets (whether Target client or not) must flow through Probe, which must be strongly capable of analyzing packets, and the throughput must be very high.

The equipment used in this paper has 40 Gbps processing performance and IO interface. The DPI server in this architecture mainly decodes the GTP communication protocol, including MSISDN-IP correspondence. The MD provides a handover interface for LEA, the X interface provided by intercept access point (IAP), e.g. MSC, SGSN, GGSN, and is usually converted into the handover interface (data format conversion); the location measurement result is fed back to LEA, and the OSNs applications for forensic analysis can be selected by MD. The following is a list of the hardware and software used to conduct the experiment:

- Tap (Net Optics 10 Gigabit iBypass Switch).
- Probe/Bypass Switch (Net Optics 10 GigaBit Fiber Taps Singlemode).
- DPI Server (NetProbe PRSN-10K).
- MITM Proxy (Dell R620 Server).
- MD (Dell R620 Server).
- Two Blackberry Torch 9800 phones (software version: 6.0 Bundle 862).
- Two iPhone 4 devices, 32GB (version 4.3.3 8J2).
- One Android phone (Samsung GT-i9000 Galaxy S—Firmware version 2.3.3).
- Facebook, Twitter, and MySpace applications for each tested phones.

5. Empirical evaluation and discussion

5.2. Inline redirection description model

Although the MITM attack is not difficult in concept, the real challenge is how to make the connection between the client and the online social network server through the MITM proxy.

In the implementation of the MITM description model, it can be divided into address resolution protocol (ARP) poisoning, web proxy, and the Inline Redirection approach, as proposed in this paper.

- In method 1, ARP poisoning, the original design of the ARP protocol is insecure, and the ARP cache is updated whenever the host receives an ARP update. Providing a sniffer is used, which pretends to be a router for a target computer (send ARP update containing router IP & sniffer MAC to target computer), it is declared to be the target computer for the router (sends ARP updates containing target computer IP and sniffer MAC to router). Afterwards, the sniffer must process all data streams between the target computer and the router, whether the data stream is encrypted or not.
- In method 2, the web proxy sets all webpage browsers, via web proxy, and is only applicable to webpage browsers. As ARP poisoning is only applicable to LAN and specific targets, in a largescale 3/3.5G network, the packet of a target smart phone cannot be led to the MITM host by ARP poisoning.

In view of this, this study proposes the Inline Redirection model. In the proposed Inline Redirection model, all traffic passes thru a very high throughput proxy (MITM proxy), which allows non-targeted traffic to pass thru the proxy without modification or interception, but manipulates the targeted encrypted traffic. The inline construction can be used for specific target smart phones, and/or specific websites or applications; furthermore, the target client's smart phone will not detect the MITM host.

5. Empirical evaluation and discussion

5.3. Scenarios

This section simulates 10 Internet fraud scenarios within Facebook, as provided by the High-tech Criminal Center, in order to evaluate the feasibility of the CloudTracker mechanism, as proposed in this paper. The criminals in these scenarios used Facebook messenger as the means of communication to avoid investigation. We select 32 Target clients (32 suspect Facebook Accounts), whose locations (GPS tracking monitoring) have been mastered by LEA, for verifying the feasibility of target SRI Location Measurement, Individualization Analysis, and historical path reconstruction.

5.4. Results summary

In Fig. 7 shows that our Inline Redirection model can defeat the encrypted content of Facebook Messenger using standard SSL/TLS encrypted communication protocol, including the user-agent:

iPhone (iOS 7.1.1), from: 100000127392962, to: 100000935848604, textline: This is Test.

Fig. 7. Decoding result of encrypted content of Facebook Messenger using standard SSL/TLS encrypted communication protocol.

5. Empirical evaluation and discussion

The 75 IP Addresses obtained from simulated scenarios (32 suspect Facebook Accounts) are used to validate the location measurement results (the base station coverage) of the Cloud-Tracker mechanism, and to match the actual locations of the Target clients (32 suspect Facebook Accounts).

Which implies to check if the GPS locations of the 32 target clients using Facebook messenger service are within the coverage of a specific base station as the results of Location Calculation Engine are. It is observed that the SRI Location Measurement results can locate the actual position of SRIs (32 suspect Facebook Accounts), and the ‘‘accuracy rate’’ is 100%, which means that the base station coverage, when a target client only knows his SRI, can be located.

In practice, it must assume that the Target client is equally likely to be at any location within that area of uncertainty. The area of uncertainty depends on the planned coverage of the base station.

For example, the 3/3.5G base station covers a radius of 150–500 m in an urban area, and 1–5 km in the suburbs. The empirical results show that the CloudTracker mechanism can successfully conduct accurate positioning and identifying, and the complete path of the target can be reconstructed, as shown in Figs. 5 and 8.

5. Empirical evaluation and discussion

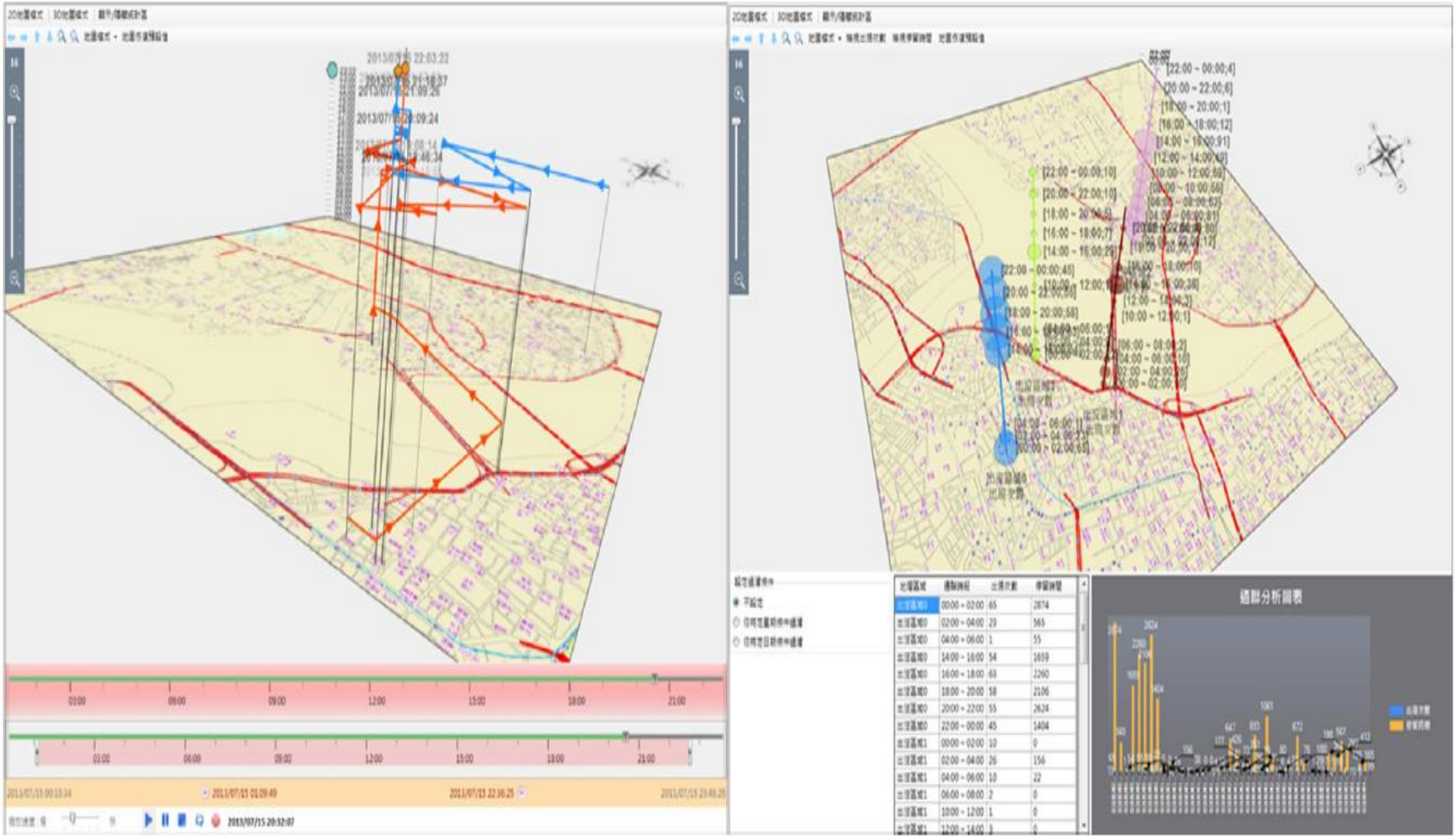

Fig. 8. Historical movement track of target client using OSNs (Cell-ID based).

6. Conclusions and future works

The proposed CloudTracker mechanism, which is based on the concepts of IP location and network forensics, develops online social network forensics tracking in the cloud. In an environment of an integrated fixed network, mobile telecommunication network 3/3.5G, and next generation network IP multimedia subsystem (IMS), each related node in the network is confirmed, the MITM proxy in charge of defeating HTTPS, while IPS (with deep packet inspection functions) is in charge of accessing, copying, decoding, and saving necessary data retention for application layer location, in order to associatively analyze the location of SRIs, and according to a given SRI, the time and information record remaining from online accessed social network applications, thus, ‘‘identity’’ can be individualized, and the complete path of the target can be reconstructed.

In terms of the contributions of this study, the application layer location of the proposed CloudTracker mechanism can be used for digital investigation in cloud-based applications. The accuracy of SRI location is from the minimum 0 m error (Internet access via fixed network) to the maximum error of cell range (Internet access via mobile network). This mechanism can also individualize the SRI, as well as target client trace reconstruction. In addition, facing the majority of social network services switching rapidly over to HTTPS versions challenges, our Inline Redirection model can solve the problems of the web proxy method and ARP poisoning method, which are only applicable to LAN and specific targets, and cannot be applied to large-scale networks. This study successfully applied it to a 3/3.5G network.

6. Conclusions and future works

In terms of implications of practice, the proposed CloudTracker mechanism does not need to modify the protocols of an existing network, redesign a new router, or set numerous reference points, as it can be directly applied to the existing network, and can provide excellent accuracy. The research findings can be used as reference for various countries to develop online social network forensics tracking, in order to effectively deal with the large number of criminal acts that can be performed through OSNs.

In terms of the limitations of this study, the proposed CloudTracker mechanism is only an applicable to domestic Internet access. In order to apply it to global Application layer location, various countries should have the same mechanism in order to meet the requirements for multinational online social network forensics tracking. For practical application of our Inline Redirection model, the processing efficiency of equipment must be good enough to undertake the data volume throughout the network. In this study, we are interested in exploring what techniques are currently available for encryption traffic. An important consideration here is the potential use of Man-in-themiddle decryption technique and Compelled certificate creation attack. Should hacking-based wiretapping technologies (Man-inthe-middle decryption technique) be used. We leave this second issue to privacy advocates, human rights activists, and legal scholars.

Q & A