Minnesota Joint Analysis Center Advisory

Office: 612-373-2840 - Fax: 612-373-2870 - Email: info@icefishx.org

Minnesota BCA Bureau of Criminal Apprehension

The Information in this overview is meant for Law Enforcement only. While none of the information contained this document pertains to a specific case the technical methods outlined in this overview could be exploited by those not bound by an oath to protect and serve.

Minnesota jac Joint Analysis Center

An Overview of VoIP for Law Enforcement

Introduction 1

What Is VoIP? 1
- Traditional Phone Systems 1
- Traditional Phone Systems Cont' 2

How VoIP Calls Are Made 2

VoIP Phones and Computers 4
- VoIP Phone 4
- VoIP Wireless Phone 4
- Application On A Computer 4

Why Use VoIP? 4

Criminal Applications 5

What Can LE Do? 5
- Tracing 5
- Identifying VoIP 5
- Caller ID 5
- Caller ID Cont' 6
- Phone Records 6
- Visual Identification 7
- Wiretapping 8

Introduction

VoIP (Voice over Internet Protocol) has become a common term for those that are familiar with telecommunications, however, it remains a mystery to many working in law enforcement.

Due to the increased use of VoIP, it is logical that law enforcement will start to encounter VoIP in the course of their investigations. VoIP allows criminals the ability to commit mass fraud, call in threats, and have secure communications, all while retaining their anonymity.

What Is VoIP?

To best describe what VoIP is and how it works, it is best to first describe how a traditional phone system works.

Traditional Phone Systems

A traditional phone system uses phone lines to make a connection to each point of the call. While the call is connected, the call maintains a continuous signal following a single route over the public telephone network.

LAW ENFORCEMENT SENSITIVE

Traditional Phone Systems Cont' For example, John wants to make a call; he picks up the phone and dials a number. That number signals the phone company to open a direct circuit to the phone number he is calling. When the other phone is answered, the circuit is complete until John or the other phone is hung up.

Cell phones work in similar fashion to traditional phone systems as they transmit and receive signals through open circuits, but data is transmitted wirelessly between phones and repeater towers. Each call follows a single, continuous route, just as a traditional telephone call does.

A circuit could be compared to a pipe. A traditional telephone call creates a single "pipe" from the caller to the call recipient. The entire call is transmitted through this same virtual pipe. When the call is finished, this virtual pipe ceases to exist. The next time the caller makes a telephone call, a new virtual pipe is created for the new phone call.

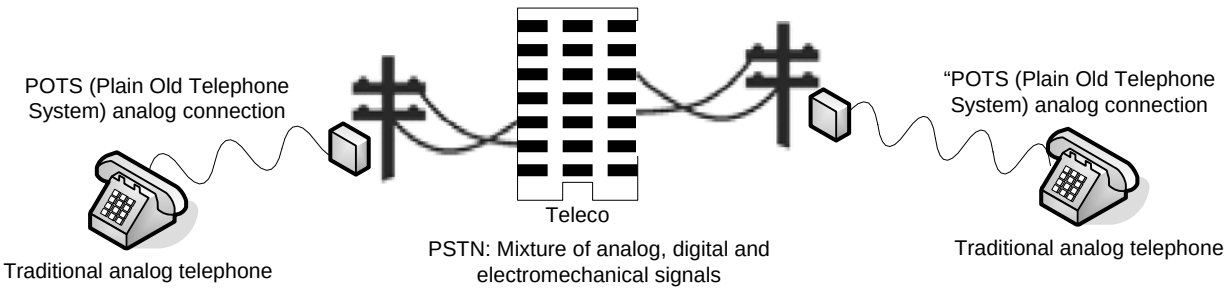

Figure 1. Example of Traditional Phone Network

How VoIP Calls Are Made: A pure VoIP telephone call originates from a VoIP phone or a computer with a VoIP software application. Voice is broken down into data packets and sent via the Internet. Unlike a traditional phone system with one connected line, the packets (now on the Internet), may travel different routes to their destination. The packets are received and reassembled into a voice signal at the receiving VoIP phone. VoIP calls don't always have to end at another VoIP type phone. Calls can be made between VoIP phones and traditional phones as well.

A digital signal is broken into small chunks of data, or "packets" that consist of 1's and 0's (digits). When a digital signal is sent over the Internet, the packets are still sent in sequence but because the packets may take different routes to reach the same destination, they may not arrive in sequence. Each packet contains a sequence number, however, so the packets can be reassembled at their destination into a signal matching the original.

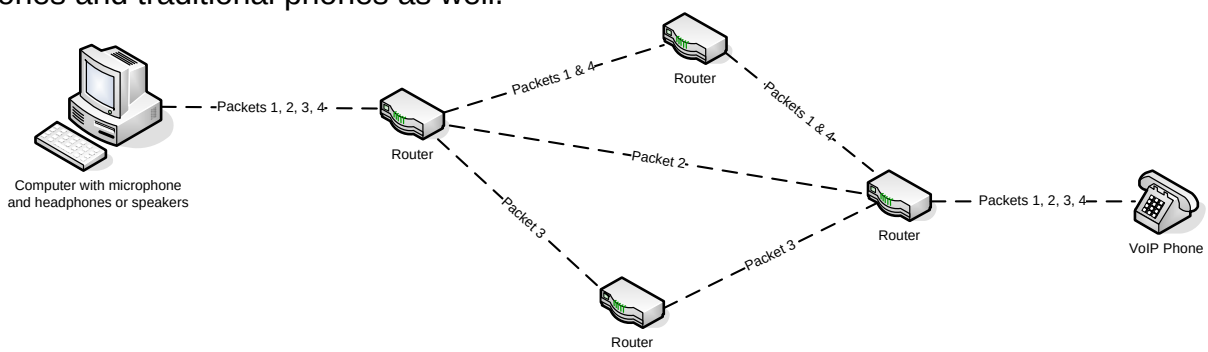

Figure 2. Example of VoIP Phone Connection

LAW ENFORCEMENT SENSITIVE

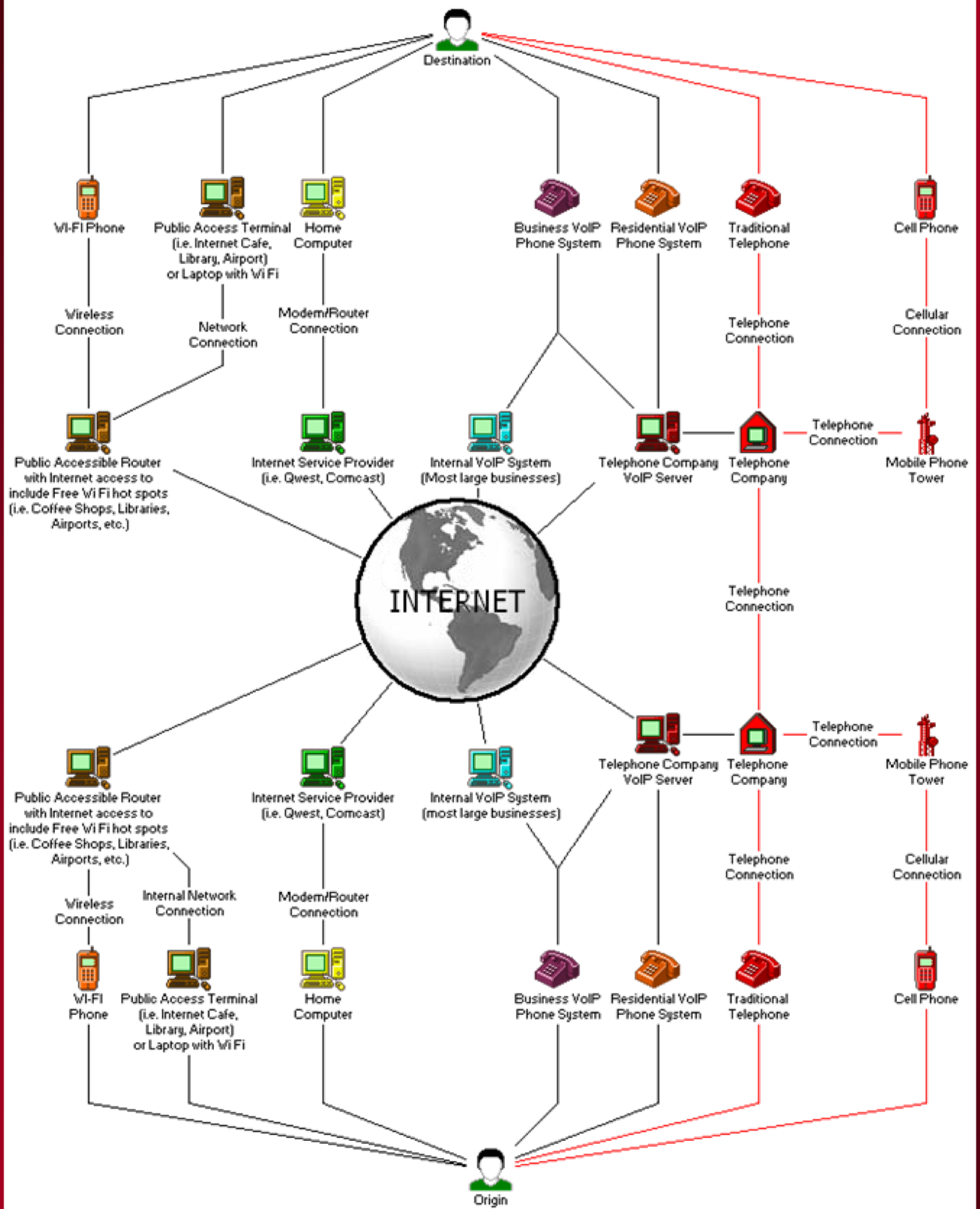

Figure 3.
Examples of Traditional and VoIP Phone Networks

VoIP Phones and Computer Applications
VoIP may make use of a mix of traditional public phone network circuits and the Internet or may be transmitted entirely via the Internet. With VoIP, there three basic ways in which to make a call: from a **VoIP phone** (or a traditional phone using a VoIP adaptor), from a **VoIP wireless phone**, or from an **application on a computer**.

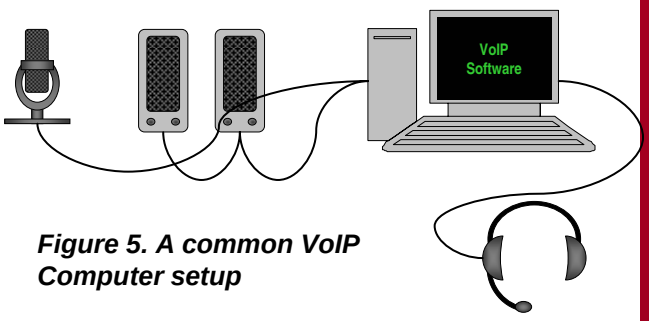

Figure 5. A common VoIP Computer setup

VoIP Phone: VoIP phones are either phones specifically designed to place calls through the Internet or traditional analog phones with adaptors that allow them to place VoIP calls using the Internet.

VoIP Wireless Phone: VoIP wireless phones work in the same manner as the previously described VoIP phone. However, connections are made through the use of wireless (also known as WiFi or Wireless Fidelity) hot spots, such as available in Internet cafes. They may also be used with wireless routers in homes or businesses.

Figure 4. A common VoIP mobile phone

Application On A Computer: The last method used to place VoIP calls is through the use of computer applications. Such applications utilize a software dialer, a microphone, and speakers on a computer to place a call. All the applications utilize the Internet and can place calls to others with VoIP software applications, VoIP phones, or even traditional phones and cell phones.

Why Use VoIP? *VoIP is becoming more popular as the technology improves and becomes more available. Some of the reasons that people or organizations are switching to VoIP are:*
1) Long distance calls are low cost or even free (with an Internet connection) as the voice signal is transmitted as data over the Internet. VoIP providers such as Vonage offer unlimited calling with flat rate plans;
2) VoIP still provides the same traditional services that have become standard such as call waiting, three way calling, caller ID, toll free numbers, and call forwarding and often provides extra features not available through traditional telephone providers.
3) When VoIP software applications such as Skype are used, calls can be placed from anywhere a high-speed internet connection is available. If the callers is traveling, the assigned number stays with the phone, as with a cell phone.
4) Additional numbers called 'virtual' or 'vanity' numbers are available in other cities, allowing people to call virtual numbers without having to pay for long distance.

LAW ENFORCEMENT SENSITIVE

Criminal Applications

There are currently three main criminal applications associated with VoIP: fraud/scams, threatening calls, and the use of some VoIP software applications for secure communications. VoIP, through the practice of "spoofing", can allow individuals to make fraudulent or threatening calls with a fake caller ID or no identifiable caller ID displayed to the recipient. In placing fraudulent calls, criminals can display the number of a legitimate organization or person in order to solicit personal data for nefarious purposes. Presenting a false caller ID number can enable an individual to make an anonymous threatening telephone call. In some cases, criminals will utilize VoIP applications to make mass computer controlled calls with an automated voice recording requesting the victim call a designated number to verify credit information, resulting in the theft of private credit or banking data; this practice is known as Vishing.

What Can LE Do?

Tracing Actively tracing a VoIP call to a source location is extremely difficult, if not altogether impossible if the VoIP user is trying to conceal his or her identity or location. Tracing VoIP calls is also difficult with emergency 911 calls. Because VoIP telephone numbers are not tied to a geographic location in the way that traditional telephone numbers are, 911 calls from VoIP phones may not be properly directed to a local dispatch center. As a result, the FCC in 2005 adopted rules that require providers of interconnected VoIP services to supply 911 emergency calling capability to their customers. (*Voice over Internet Protocol (VoIP) and 911, FCC Public Safety & Homeland Security Bureau*, http://www.fcc.gov/pshs/services/911-services/voip/Welcome.html.)

VoIP E911 was developed to allow VoIP providers in the U.S. the ability to support emergency services. The VoIP E911 emergency-calling system associates a physical address with the calling party's telephone number as required by the Wireless Communications and Public Safety Act of 1999. However, subscriber participation in E911 is not required and VoIP users can opt-out or disable E911 service on their lines if desired. This example demonstrates that if an individual using VoIP does not want to be identified or located, attempting to trace a VoIP call is unlikely to yield positive results.

Identifying VoIP

In the course of an investigation in which VoIP has been suspected as part of a crime, being able to identify VoIP components for a search warrant or seizure is vital. There are four parts to identifying VoIP: VoIP phone calls with caller ID, VoIP phone calls on phone records, VoIP phones and associated hardware, and VoIP software on computers.

Caller ID - When attempting to identify a VoIP call based on caller ID, be aware that the caller ID presented number may appear the same as any other common telephone number. obscuring whether the call was placed using a traditional phone system or a VoIP system. However, if a caller is intentionally masking (or spoofing) a phone number, a false number may be displayed. Phone numbers that do not associate with regulated number guidelines (i.e. movie numbers, 555-XXXX, etc.) may indicate that the call was VoIP originated and changed via masking, or spoofing. Of course, spoofing can also change numbers to appear legitimate in order to throw blame onto another person or organization.

LAW ENFORCEMENT SENSITIVE

Caller ID Cont' - Number masking is also a common and legitimate practice used by many businesses and government entities that use their own internal telephone systems. Call numbers can be masked or changed on the caller ID appearance of outgoing calls. For instance, a company may want all outgoing calls from its employees to appear as if they came from the company's main telephone number, no matter what the employee's actual phone number is. A government agency may choose to mask its outgoing telephone numbers to obscure its identity.

Phone Records **-** Records from the phone company will not indicate that the number is from a VoIP system. Traditional telephone providers, VoIP providers, cell phone providers, and businesses or organizations can purchase blocks of phone numbers from telecommunications companies. The subscriber information on those numbers may be associated with a legitimate entity that can be located; or the numbers may be associated with a company that utilizes that number as a "conduit" for multiple users. At this point, tracing the call becomes more like tracing an email. A separate request / subpoena must be written to get the information from the VoIP provider. Many providers are incorporated outside of U.S. jurisdiction and therefore do not have to fulfill the request. If the provider does honor the request, in most circumstances it will provide the account information, which will include payment information and may or may not include the following: name, address, email address, IP address where the account was accessed. Theoretically, the VoIP provider could have records of other calls placed by the subscriber; however, most companies will not retain those records because of the data space required.

The payment information could be like any e-commerce purchase method used with the email address (credit card, money order, electronic funds transfer). Obtaining the account information will depend greatly on the provider.

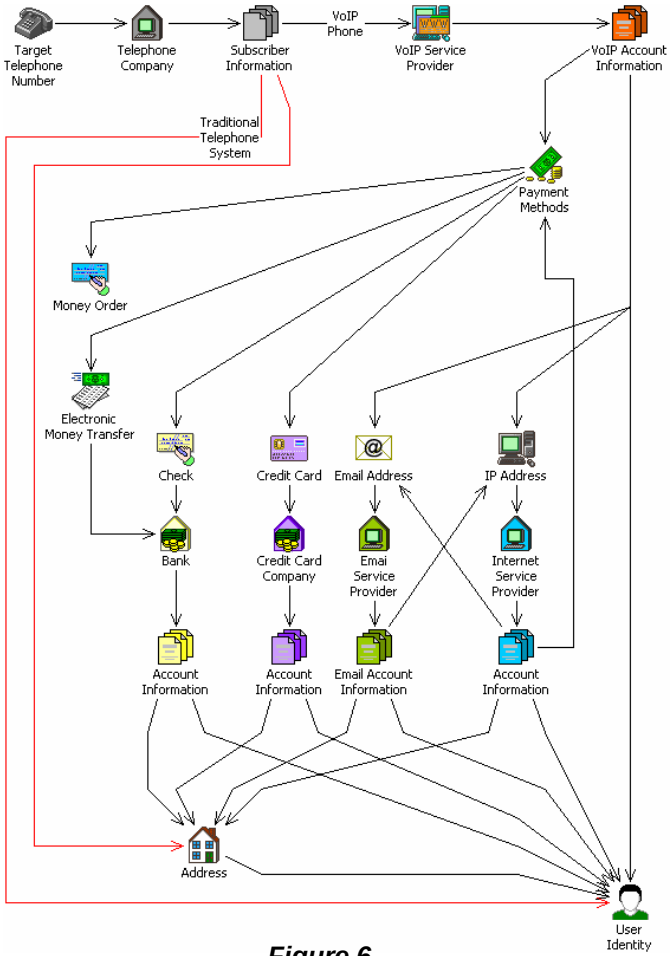

Figure 6.
Associating a telephone Number to an Identity

LAW ENFORCEMENT SENSITIVE

Visual Identification **-**The difference between VoIP phones and traditional phones can be subtle. Consider the following when trying to locate VoIP phones:-Traditional phones utilize cables with RJ-11 connectors, whereas VoIP phones will utilize cables with RJ-45 connectors (fig 8).

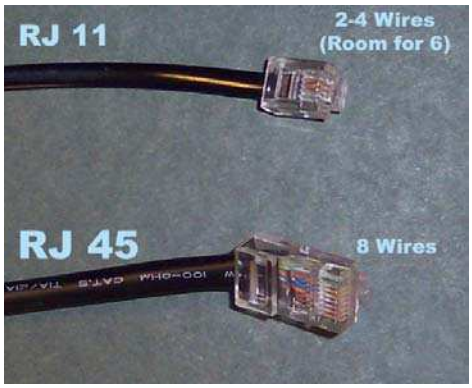

Figure 7. Cable Comparison

-Traditional phones will continue to work if a home or business's electrical power is unavailable because the telephone company's switches provide the signaling power for traditional calls. VoIP phones must get their electrical power directly from the home or business that is using VoIP. Power can be supplied to the phone with a power adapter by plugging the phone into an electrical outlet, or via an RJ-45 cable. Most home VoIP systems will not have this capability but many business VoIP systems will.

-Traditional analog phones can become VoIP capable with the use of a VoIP analog adaptor. Trace the phone cord from a traditional phone; if the cord is connected to a device that is then connected to a computer or other networking hardware device, such as a a cable modem or DSL-modem, the phone has been adapted for VoIP use (fig 7).

-VoIP mobile phones are difficult to differentiate from traditional cell phones by the untrained eye (fig 4). Turn over suspected VoIP mobile phones to technical personnel for further inspection.

-Personal computers, both laptops and desktops can be utilized for VoIP as long as they have Internet connectivity. A computer with a microphone connected can also be a sign that VoIP is being used, However, only an inspection of the applications installed on the computer will definitively confirm the presence of VoIP software. A partial, but significant common VoIP software applications can be found at:
http://en.wikipedia.org/wiki/Comparison_of_VoIP_software

Figure 8.
Displays an example of a VoIP setup utilizing an adaptor

LAW ENFORCEMENT SENSITIVE

Wiretapping In September 2005, the FCC issued an order requiring VoIP providers to comply with the Communications Assistance for Law Enforcement (CALEA) Act of 1994, which previously applied to traditional phone companies but not VoIP providers. CALEA requires that VoIP carriers provide law enforcement agencies the means, with the proper warrants, to tap into and record voice conversations and to trace the source and destination of calls made through the carrier's networks. However, due to the international nature of the Internet, it may be impossible to legally wiretap conversations that are supported by foreign VoIP offering companies.

Compiled by the MNJAC with assistance from BCA Tech Support.
If you have any questions, concerns or feedback, please contact MNJAC at 612-373-2840 or info@icefishx.org

LAW ENFORCEMENT SENSITIVE