韓國컴퓨터情報學會 論文誌
第14卷 第5號, 2009. 5.

2009-14-5-4-1

WiBro 네트워크에서 메신저, VoIP 도청 및 포렌식 연구

천 우 성*, 박 대 우**

A Study of Forensic on Eavesdropping from VoIP and Messenger through WiBro Network

Woo-Sung Chun*, Dea-Woo Park**

요 약

우리나라 WiBro가 IEEE 802.16e로 국제표준화 되어 수도권부터 WiBro 네트워크 사업을 수행하고 있다. 본 논문에서는 WiBro 네트워크에서 빈번하게 일어나는 메신저 프로그램과 VoIP를 통한 음성 및 화상 통화에 대해 도청을 실시하였다. 패킷 수집과 분석기인 와이어샤크를 통해서 패킷의 도청을 실시하고 SIP, H.263, TCP, UDP 프로토콜을 바탕으로 도청자료를 재생한다. 패킷이 위변조 되지 않았다는 무결성을 시간을 기준으로 검증하여 도청된 VoIP 음성 패킷의 복사본의 시간과 패킷의 시간 그리고 X-Lite 통화 기록의 시간이 일치함을 증명하여 무결성을 검증한다. 무결성이 검증된 자료는 밀봉 봉투에 넣어서 수사 자료로서 활용하기 위해 밀봉 후에 수사관의 간인을 실시하여 법정에서의 증거자료로 사용 할 수 있도록 준비한다.

Abstract

Korean WiBro becomes international standard to IEEE 802.16e, and We are carrying out a WiBro network business from capital regions. We executed eavesdropping about voices and messenger program and the VoIP which frequently happened in WiBro networks at these papers. We have a lot in common with the Wireshark which is a packet collection and an analyzer, and We execute eavesdropping, and We reproduce eavesdropping data with bases to a SIP, H.263, TCP, UDP protocol through packets. In time of a copy of a packet negative the VoIP which verify time with bases, and was eavesdropped on integrity packet and a X-Lite call record, be matched that a packet is counterfeit forgery did not work, and We demonstrate, and verify integrity. The data which integrity was verified put in a seaming envelope, and we prepare so as it is to a liver of investigator, and execute, and to be able to do use to proof data after seaming in courts in order to utilize as criminal investigation data.

▸ Keyword : Eavesdropping, Forensics, Packet Analysis, WiBro Network

• 제1저자 : 천우성(deux8522@nate.com), 교신저자 : 박대우(prof1@paran.com)
• 투고일 : 2009. 05. 11, 심사일 : 2009. 05. 13, 게재확정일 : 2009. 05. 27.
* 호서대학교 벤처전문대학원 IT응용기술학과 ** 호서대학교 벤처전문대학원 교수

Ⅰ. 서 론

WiBro(Wireless Broadband Internet)[1]는 2.3GHz 주파수 대역을 이용하며 이동단말이 60km/h이상 이동 시에도 가입자당 전송속도 약 1Mbps의 끊김없는(seamless) 휴대인터넷 서비스를 제공한다. WiBro 서비스는 Wireless MAN (Metropolitan Area Network)에서 출발하여 수신안테나와 가입자 장치(Subscriber Station)를 이용한다. 상용 케이블모뎀은 표준규격인 DOCSIS (Data-Over-Cable Service Interface Specification)을 근간으로 LOS(Line-of-Sight) 통신환경에서 PHY 모드인 OFDM, OFDMA와 MAC 규격에서 IEEE 802.16e 표준화가 추진되었다.

IEEE Std. 802.16-2004(TGd Specification)는 역방향 호환성(Backward Compatibility)을 유지하면서, 단말기의 이동성을 지원하기 위한 표준화 작업을 하고 있다. 역방향 호환성의 의미는 고정형 규격을 지원하는 가입자 이동단말은 이동성을 지원하는 기지국에 의하여 서비스가 제공되어야 한다는 것과, 이동성을 지원하는 가입자 이동단말은 이동성을 제한하였을 때 고정형 기반의 기지국에 의하여 서비스가 제공될 수 있어야 한다는 것이다.

공격자인 해커는 이러한 역방향 호환성을 이용하여 WiBro 이동단말에서 빈번하게 사용되는 메신저(Messenger)와 VoIP 서비스 등에 대한 불법적인 공격을 하여, 사회업무 및 금융거래 등의 목적시스템에 대한 악의적인 직·간접의 피해를 줄 수 있다. 해커는 휴대인터넷인 WiBro 서비스의 이동단말의 이동성을 이용하여 추적을 따돌리고 신속한 업무와 금융거래 정보 등의 도청으로 안전을 위협한다.

이러한 해커의 불법적인 행위에 대한 안전성과 보안성을 강화하고, 국가 법질서 수호를 위해 필수적으로 요구되는 것이 WiBro 이동단말 공격에 대한 패킷의 분석과 이를 통한 IP 역추적을 위한 모바일 포렌식의 자료를 생성하는 것이다. 이러한 포렌식 데이터의 분석을 통해 과학적이고, 증거에 의한 객관적인 수사를 할 수 있으며, 수사한 결과로서 포렌식 자료는 법정에서 책임과 판단의 증거자료로 사용되어질 것이다.

본 논문의 관련연구에서 휴대인터넷인 WiBro에 대한 표준화 규격 및 기술 절차를 연구한다. 또한 WiBro 환경에서 무선인터넷을 실행하고 VoIP(Voice of Internet protocol)[2]나 메신저[3]를 사용하여 패킷을 수집하고 분석하여, VoIP에서 음성의 도청[4]과 메신저에서의 채팅 내용을 재생하여 보여줌으로서, 본 논문을 통하여 포렌식 자료를 도출[5]하고, 생성하는 것에 대한 기술을 연구한다.

Ⅱ. 관련 연구

본 장에서는 연구에 사용된 WiBro 시스템에 설치할 패킷 분석 툴 프로그램들의 종류와 기능 및 VoIP 도청 및 메신저 내용을 도청하고 포렌식 자료 생성[6]에 필요한 관련연구를 한다.

2.1. WiBro

WiBro 규격은 IEEE 802.16-2004 및 IEEE P802.16e/D3 또는 이후 버전으로서 이중화 방식은 TDD(Time Division Duplexing)을 사용하고, 주파수 재사용계수는 1을 만족하여야 하며, 채널대역폭은 9MHz 이상을 가지고, 이동성 시속 60km/h 이상에서 셀 간의 경계구역에서 최소 전송속도 UL 128 kb/s, DL 512 kb/s를 만족하여야 하며, 사업자간 로밍을 제공하여야 하는 등의 5가지 요구사항을 만족하여야 한다.

국제 표준으로 확정된 IEEE 802.16e에서는 이동성을 지원하기 위하여 Handoff 및 Sleep Mode 기능 제공뿐만 아니라, 단말기의 절전 기능을 극대화시키며 광역에서 기지국간 안정성 있는 멀티캐스트/브로드캐스트 서비스를 제공하기 위한 MBS(Multicast & Broadcast Service) 및 Idle Mode 기능, 착신 서비스를 고려한 Paging 기능, 그리고 보다 빠른 핸드오버를 제공하기 위한 FBSS(Fast Base Station Switching) 기능 등이 표준에 반영되었다. 또한 시스템의 성능을 향상시키기 위한 다중안테나 관련 기술인 AAS(Adaptive Antenna System) 및 MIMO(Multiple-Input Multiple- Output)들이 다수 제안되고 채택되었다. 최근에는 보다 개선된 Channel Coding 방식인 LDPC 기술 등도 채택됨으로써 보다 다양한 기능을 제공한다.

2.2. 메신저

현재 컴퓨터 매개 커뮤니케이션(CMC:Computer Mediated Communication)중에서도 빈번히 사용되고 있는 것이 인스턴트 메신저(Instant Messenger)로서, 전화나 이메일 이상으로 사용빈도가 높은 커뮤니케이션 채널로 발전하고 있다. 우리나라에서는 네이트 온(Nate On)과 Windows Live Messenger(WLM)가 가장 많이 사용된다.

2.3. VoIP

그림 1에서와 같이 기존의 인터넷 서비스 사업자들이 구축

한 인터넷 네트워크를 이용한다. 최근에는 VoIP 서비스가 단순히 값싼 요금의 전화 서비스 제공에 머물지 않고 음성과 데이터를 통합한 부가 서비스 제공에 역점을 두는 추세이다.

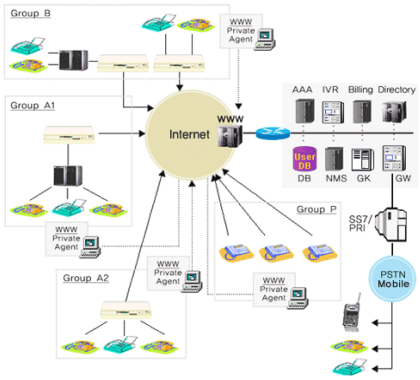

그림 1. 인터넷 VoIP 서비스
Fig 1. VoIP Service on Internet

VoIP는 인터넷의 IP 계층을 사용하여 음성을 전송하는 기술을 말하며 다른 용어로 인터넷 전화와 혼용되어 사용된다. VoIP는 아날로그의 신호를 디지털 신호로 변환한 후, 패킷으로 구성하여 IP네트워크인 인터넷을 통해 인증[7]한 후 수신측까지 전달하는 것을 의미하지만, 인터넷 전화는 IP 네트워크 뿐 만 아니라, 음성과 팩스 데이터를 전송할 수 있는 모든 네트워크(ATM, Frame Relay)에서 기존 전화네트워크에서 제공하는 서비스를 지원한다.

2.4. SIP(Session Initiation Protocol)

SIP 프로토콜은 VoIP 사용자의 세션을 생성하고, 수정하고, 종료하기 위한 응용 계층의 call signaling 프로토콜[8]이다. call signaling을 위해 SIP프로토콜을 사용하는 전체적인 네트워크 구성도는 그림 2와 같다.

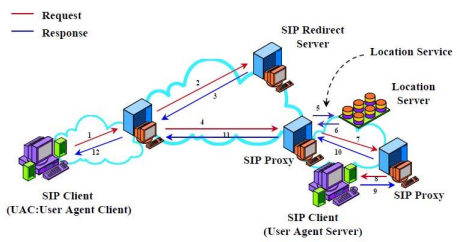

그림 2. SIP 네트워크 구성도
Fig 2. SIP network formation

SIP를 이용하여 세션 연결 설정을 하기위해서는 통신의 주체로 SIP요청 메시지를 생성하는 UAC(User Agent Client)와 수신된 요청 메시지에 응답하는 UAS(User Agent Server)로 동작한다. UAC가 call을 요청하는 INVITE 메시지를 UAS에게 전달해 주는 기능을 한다. Proxy server는 요청받은 INVITE 메시지를 목적지까지 포워딩 해주는 역할을 하며, Redirect server는 UAS에 대한 정보를 UAC에게 전달해 주어 UAC가 UAS에게 직접 INVITE 메시지를 보낼 수 있도록 해주는 역할을 한다. 링크사용자는 Registrar server에 REGISTER 메시지를 전송함으로 자신의 위치정보를 Location server에 등록할 수 있다. UA의 실질적인 위치를 저장하고 있는 서버이다.

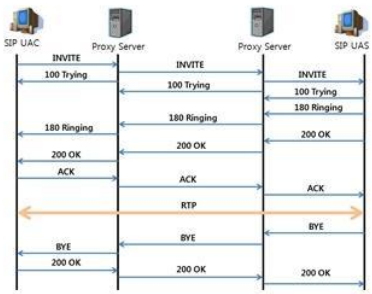

그림 3. SIP 프로토콜 세션 설정 및 종료
Fig 3. SIP protocol session setting and end

두 단말간의 음성 통신을 위하여 SIP 프로토콜을 사용하여 사용자간의 세션을 설정하고, 종료하는 과정[9]은 그림 3과 같은 절차에 의해 이루어진다.

2.5. 패킷 캡처 및 분석 프로그램

Ethereal은 Unix와 Windows에서 동작하는 Network Protocol Analyzer이다. Ethereal과 이후에 와이어샤크(Wireshark)[9]을 사용하여 현재 동작하는 네트워크 혹은 시스템에서 캡처되어 저장된 파일을 통해서 각각의 패킷에 대한 세부적인 데이터를 분석할 수 있다.

무선 인터넷을 할 때에는 AP(Access Point)와 단말기가 MAC을 통해 IP, TCP, UDP 등과 같은 프로토콜을 통해서 정보를 주고받게 되는 정보 패킷을 캡처한다.

SIPTAP이라는 소프트웨어는 인터넷전화를 해킹, 원격지에서도 통화내용을 도청하고 녹음까지 가능하다.

Cain & Abel[10]은 와이어샤크와 유사한 기능을 갖는 패킷 캡처 프로그램으로 패킷의 재생도 가능하다.

III. 메신저와 VoIP 도청

WiBro 네트워크 환경에서 일반적으로 많이 사용하는 Messenger의 채팅과 화상전화 및 VoIP 전화가 도청됨을 밝히고, 포렌식 자료를 생성한다.

3.1. WiBro환경에서 메신저 설치

WiBro는 서비스를 위한 USB형식의 모뎀은 휴대성과 모뎀을 내장하여 인터넷을 연결하는 휴대용 인터넷이 가능하다. 통신을 하고자하는 단말에 프로그램을 설치하면 인터넷에 연결된다. 그림 4와 같이 접속 프로그램을 실행하여 인터넷에 연결한다.

그림 4. WiBro 접속 화면
Fig 4. WiBro accessed screen

3.2. 메신저에서 실시간 문자 채팅

세계에서 보편적으로 많이 사용되고, 우리나라에서도 많이 사용되는 WLM이고 윈도우 운영체제에서 기본적으로 제공하는 프로그램이기도 하다. MSN 메신저의 실시간 채팅 도청실험에서는 저작권의 문제도 있어 우선 도청할 상대의 MSN 메신저를 통해 채팅을 할 때, 와이어샤크를 실행하여 패킷 수집을 하면, 상대편의 현재 유동 IP 주소를 알아내어 실험한다.

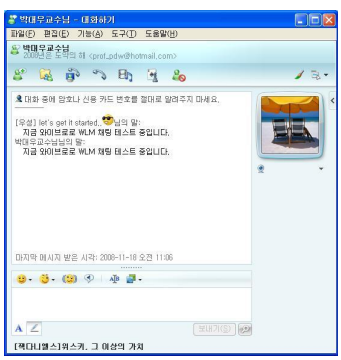

그림 5. WLM 문자 채팅
Fig 5. WLM Character chatting

3.3. 메신저에서 화상전화

WLM의 메신저프로그램에서 기본적으로 제공되는 기능 중에 하나가 화상전화기능으로 웹캠과 마이크가 있어야 하며, 그림 6처럼 화상전화를 하였다.

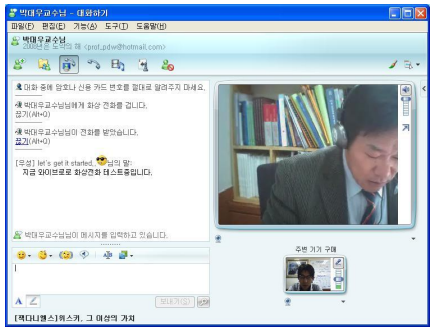

그림 6. WML 화상전화 연결
Fig 6. WML video-telephone connection

3.4. VoIP 전화

3.4.1 WiBro 네트워크 VoIP 실험 환경

WiBro 네트워크에서 VoIP 도청 실험 환경은 그림 7과 같다.

(통화자 1) PC SPEC - O.S. Microsoft Windows XP Professional V2002, Service Pack 2, CPU Intel Core2 6400 2.13Ghz, RAM 2GB, HDD 300GB이다.

(통화자 2) 노트북 SPEC - O.S. Microsoft Windows XP Home Edition V2002, Service Pack 2, CPU Genuine Intel T2400 1.83Ghz, RAM 1GB, HDD 30GB이다.

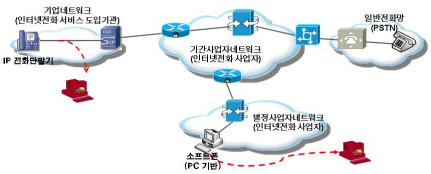

그림 7. WiBro 네트워크 VoIP 도청 실험 환경
Fig 7. WiBro network VoIP Eavesdropping experiment environment

3.4.2 Packet 분석기 설치

Cain & Abel을 http://www.oxid.it에서 Windows XP용 v4.9.23을 다운받아 Victim WiBro 이동 단말기와 Attacker의 WiBro 이동 단말기에 WinPcap과 함께 설치하였다. Wireshark을 http://www.wireshark.org에서 Windows XP용 v1.0.4 을 다운받아 WinPcap과 함께 Victim, Attacker의 WiBro 이동 단말기에 설치하였다.

3.4.3 VoIP 소프트 폰 설치

VoIP는 기본적으로 인터넷을 바탕으로 이루어지므로 WiBro 네트워크에서 인터넷이 연결되어 있어야 한다. VoIP 전화는 USB형식의 전화기를 연결하여 전화를 할 수 있는 형식과 소프트폰으로 인터넷에 별도의 프로그램을 설치하여 사용하는데, 상용 프로그램들은 저작권과 소송의 위험이 있어서 그 중 X-Lite[11] 네이버폰을 실험 대상으로 한다. VoIP가 윈도우에서도 SIP 프로토콜을 기반으로 사용하는 VoIP 전화로 같은 기능을 수행하는 프로그램들 중에서 X-Lite를 사용하였다. VoIP 전화번호는 *8009 4455와 *8005 8522 번호를 부여받았다[12]. 그림 7에서는 X-Lite를 이용하여 음성 및 화상으로 전화연결을 하였다.

그림 8. X-Lite 소프트 폰 통화 설정
Fig 8. X-Lite soft phone call setting

3.5. 패킷수집

WiBro 네트워크 환경에서 패킷수집을 위해 프로그램을 구동한다. 와이어샤크 프로그램을 웹사이트에서 다운받아 설치한다. 와이어샤크에 메뉴바에서 Capture 탭에 Interfaces 항목을 선택하면 자신의 시스템에 있는 NIC 정보를 확인하고 선택하여 패킷을 수집을 시작한다.

윈도우환경에서 패킷을 수집하기 위해 기본적으로 WinpCap을 공유기 근처에 설치하여야 하고 분석작업을 위해 와이어샤크를 설치한다. 와이어샤크와 WinpCap은 서로 연동이 되어 패킷을 수집하고 그것을 분석한다. 그림 9와 같이 패킷을 수집한다.

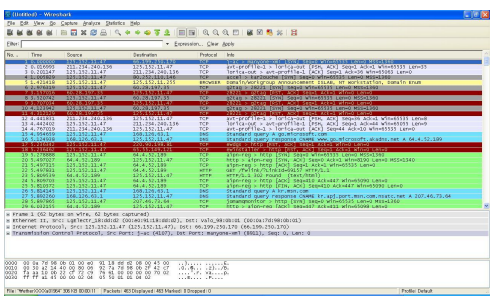

그림 9. 와이어샤크 패킷 수집
Fig 9. WireShark packet collection

3.6. Messenger 문자 채팅 도청

WiBro 네트워크 환경에서 WLM를 사용하여 실시간 문자 채팅을 실시한다. 패킷 수집 프로그램 툴인 와이어샤크를 이용하여 접속 처음부터 패킷을 수집한다. WLM 실행 전 와이어샤크를 실행하여 패킷 수집을 위한 준비를 한 후 WLM을 실행한다.

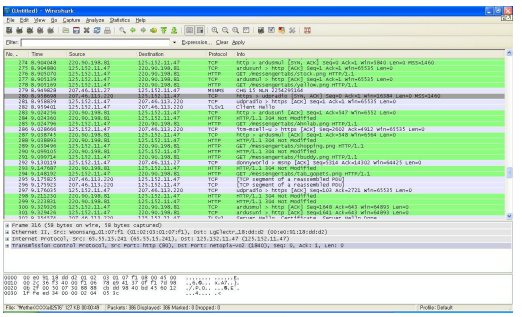

그림 10. WLM 통신으로 수집된 패킷
Fig 10. Collected packets by WLM communication

3.7. 메신저 화상 전화 도청

문자채팅에서 패킷을 수집한 방법과 같이 와이어샤크를 먼저 실행하여 패킷수집을 준비하고 WLM을 실행한다. WLM에 기능중 하나인 화상전화 기능을 사용하여 화상전화를 한다. Messenger에서 음성과 영상은 UDP패킷으로 전달하기 때문에 와이어샤크에서 패킷 수집 정보 중 UDP패킷을 분석하게 된다.

3.8. VoIP 전화 도청

WiBro를 실행시켜 인터넷을 접속한다. WiBro 네트워크 환경에서 와이어샤크를 실행시켜 패킷 수집을 준비하고 VoIP를 하기 위해 소프트 폰인 X-Lite를 실행한다. X-Lite로 상대편 번호로 전화를 걸면 와이어샤크에서 패킷을 수집하게 되고 SIP 프로토콜을 통해 음성 및 Data 패킷으로 잡히는 것을 알 수 있다. 화상전화는 H.263 프로토콜을 이용하여 실시간으로 전송된다.

VoIP 음성통화는 SIP 프로토콜 수집기인 와이어샤크에서 SIP Calls라는 기능을 사용하여 음성패킷을 수집하고 실행시킨다. 와이어샤크로 패킷을 수집하고 수집이 끝나면 메뉴에 Statistics탭에서 SIP Calls을 설정하고, VoIP 패킷이 수집된 것을 확인한다.

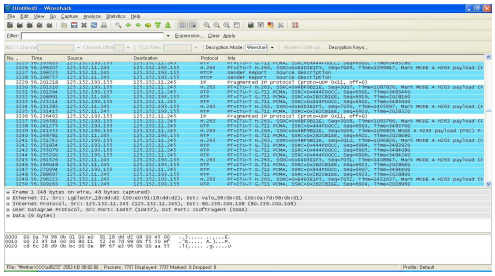

그림 11. VoIP 패킷 수집
Fig 11. VoIP packet collection

IV. 도청 분석과 포렌식 자료 분석

WiBro 네트워크 환경에서는 유동 IP를 사용하여 인터넷 연결을 하므로, 패킷 수집을 하기 위해선 상대방의 IP를 알아야 한다. 도청할 대상의 상대편 정보는 유동이기 때문에 IP가 새로 접속할 때마다 바뀌므로 그 점을 고려[13]해야 한다.

4.1. 도청자료 재생 및 원본 비교

와이어샤크에서 수집된 패킷을 바탕으로 하여 도청된 MSN 메신저의 패킷 중에서 Follow TCP Stream, Follow UDP Stream을 통하여 자료 중에서 영문과 숫자로 된 내용이 도청됨을 확인 하였고 원본과 비교 내용이 일치 하였다.

그러나 동영상에 대한 도청을 실시하였으나, 동영상 전송에 따른 도청은 성공하지 못하였다.

VoIP 전화 도청자료의 재생을 위하여 와이어샤크의 메뉴 탭에서 Statistics탭을 누르고 SIP Calls를 실행하면 수집된 패킷 중에 SIP기반으로 하여 VoIP를 사용한 패킷만 검색이 된다. 그 검색 패킷을 선택하고 Player버튼을 부르면 Decode를 하게 된다. Decode가 끝나면 그림 12와 같이 음성신호가 잡힌 것을 알 수 있다.

음성 신호를 Play하여 음성 재생을 확인하였다. 즉 실험실 환경에서 도청이 가능하여 원래 음성정보가 재생되었다.

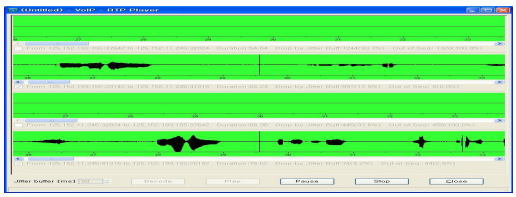

그림 12. 와이어샤크에서 VoIP 음성 패킷 재생
Fig 12. VoIP voice packet revives at Wireshark

4.2. 포렌식 자료 생성

와이어샤크에서 수집한 패킷과 재생했던 도청자료를 도청된 패킷의 데이터 시간과 휴대폰의 시간을 일치 시키는 사진을 수록하고, 패킷은 더 이상 변조 되지 않는 복사본[14]을 만들어 보관한다. 도청된 VoIP 음성 패킷의 복사본의 시간과 패킷의 시간, 그리고 X-Lite 통화 기록의 시간이 일치함을 증명하여 무결성을 검증한다. 이러한 포렌식 과정을 통하여 무결성을 증명하게 되면 법적 효력이 있는 증거자료로 생성된다.

MSN 메신저의 패킷의 시간을 확인하고 휴대폰의 시간 기록과 일치됨을 사진으로 만들어 확인하도록 한다. 또한 VoIP 음성 패킷의 복사본의 시간과 패킷의 시간, 그리고 X-Lite 통화 기록의 시간이 순서상으로 일치됨을 증명하여 무결성을 검증한다.

무결성이 검증된 자료는 밀봉 봉투에 넣어서 수사 자료로서 활용하기 위해 밀봉 후에 수사관의 간인을 실시하여 법정에서의 증거자료로 사용 할 수 있도록 준비한다.[15]

4.3. 연구 결과의 비교 분석

도청의 문제는 사회적으로 민감한 문제이므로, 연구실 내의 WiBro 네트워크를 이용하여 실험을 실시하였다. 그리고 통제된 환경에서 WiBro에서 빈번히 사용되는 일반적인 프로그램을 이용하였다. 연구 분석의 결과는 표1과 같다. VoIP 서비스의 음성은 재생이 가능 하였고, 영상은 일부분만 도청이 가능하고 재생되었다. 메신저인 WLM은 영어로 된 문자 채팅의 내용 도청은 가능하였으나, 한글로 된 내용은 도청 재생이 확인 불가하였다.[16]

표 1. 기존 연구와 비교분석
Table 1. Comparative analysis

	Service	본 연구
VoIP 서비스	음성	음성재생 도청 가능
	영상	영상재생 일부 가능
메신저 (WLM)	한글	한글내용 확인 불가
	영문	영문내용 확인 가능

V. 결 론

본 논문에서는 IEEE 802.16e로 국제표준화 되어 수도권부터 WiBro 네트워크 사업을 수행하고 있는 WiBro 네트워크 환경에서 이동단말 네트워크 시스템에서 메신저의 화상채

팅과 VoIP전화의 음성 및 화상 도청을 실시하였고 패킷을 분석하여 무결성을 검증하여 포렌식 자료를 생성 하였다.

WiBro 네트워크 환경에서 가장 빈번하게 일어나는 메신저 프로그램과 VoIP를 이용한 음성 및 화상 통화에 대해 도청을 실시하였다. 패킷 수집기인 와이어샤크에서 수집한 패킷을 통해 도청을 실시하고 SIP, H.263, TCP, UDP 프로토콜을 바탕으로 도청자료를 재생하여, 패킷이 위변조 되지 않았다는 무결성을 시간을 기준으로 검증하여 법적 효력이 있는 모바일 포렌식 증거자료를 제시하게 된다.

이로서 WiBro 네트워크 환경에서 침해사고가 발생 하였을 때, 불법적인 행동에 대한 책임을 판단할 포렌식 자료를 생성하고, 이 자료를 통한 WiBro 이동단말과 IP 역추적과 함께 보안 감사 자료로써, 모바일 포렌식 자료나, 이동단말 포렌식 자료를 생성하여 전체적인 WiBro 이동단말 네트워크 시스템의 안정성 확보와 보안성 강화를 위한 연구를 할 수 있다.

향후 연구에서는 유비쿼터스와 IPv6 환경에서의 이동단말 사이에서 실시간 도청 및 해킹을 당하였을 경우 WiBro 이동단말과 IP 역추적 실시에 대한 기술과 포렌식 방법론에 대한 연구가 필요하다.

참고문헌

〔1〕 KT WiBro homepage, *http://www.ktWiBro.com/ktWiBro/main.html*, November 2008.

〔2〕 VoIP 기술 동향, 〔IITA〕 정보통신연구진흥원 학술정보, 주간기술동향 1021호, 2008년 09월.

〔3〕 Windows Live Messenger homepage, *http://windowslive.msn.co.kr/wlm/messenger/*, Nov. 2008.

〔4〕 박대우, 윤석현, "VoIP 서비스의 도청 공격과 보안에 관한 연구," 한국컴퓨터정보학회논문지, 제 11권, 제4호, 155-164쪽, 2006년 9월.

〔5〕 B. Williamson, *"Forensic Analysis of the Contents of Nokia Mobile Phones"*, School of Computer and Information Science Edith Cowan University Perth, 2005.

〔6〕 V. Luoma, "Forensics and electronic discovery: The new management challenge," Computers & Security, 25(2), pp.91-96, 2006.

〔7〕 안영두, 이순흠, "SIP 기반 유무선 통합 컨퍼런스 시스템 개발," 한국정보기술학회논문지, 제 5권, 제 3호, 2007년 09월.

〔8〕 장유정, 정수환, 문형권, 최재덕, 원유재, 조영덕, "SIP 기반의 VoIP 서비스 환경에서 스팸 방지를 위한 인증 기법," 한국통신학회논문지, 제 32권 제 8호(네트워크 및 서비스), 2007년 08월.

〔9〕 Wireshark is 1.0.5, Get Wireshark, *http://www.wireshark.org/download.html*, November 2008.

〔10〕 Download Cain & Abel v4.9.26 for Windows NT/2000/XP, *http://www.oxid.it/cain.html*, November 2008.

〔11〕 Download X-Lite 3.0 for Windows, *http://www.counterpath.net/X-Lite-Download.html*, November 2008.

〔12〕 대한민국 대표 무료전화 아이엠텔, *http://www.imtel.com*, 2008년 11월.

〔13〕 박상락, 컴퓨터포렌식과 디지털증거의 분석, 컴퓨터수사와 정보보호, 203-204쪽, 2003년 9월.

〔14〕 P. Kanellis, E. Kiountouzis, N. Kolokotronis & D. Martakos(Eds.), *"Digital crime and forensic science in cyberspace"*, Journal of digital forensic practice, Hershey : Idea Group, 2006.

〔15〕 박대우, 임승린, "WiBro에서 공격 이동단말에 대한 역추적기법 연구," 한국컴퓨터정보학회논문지, 제12권, 제3호, 185-194쪽, 2007년 7월.

〔16〕 Dea-Woo Park, "A Study of Packet Analysis regarding a DoS Attack in WiBro Environments", International Journal of Computer Science and Network Security, IJCSNS (1738-7906), Dec. 2008.

저 자 소 개

천 우 성

2006년 숭실대학교 전산원 졸업
2006년 한국교육개발원 멀티미디어학 전공 (공학사)
2008년 호서대학교 벤처전문대학원 IT응용기술학과 (석사과정)
〈관심분야〉 정보보호, 소프트웨어 감정평가, 추적기법, 유비쿼터스 보안, 소프트웨어 포렌식 등

박 대 우

1998년 숭실대학교 컴퓨터학과(공학석사)
2004년 숭실대학교 컴퓨터학과(공학박사)
2000년 매직캐슬정보통신 연구소 소장, 부사장
2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2006년 정보보호진흥원(KISA) 선임연구원
2007년 호서대학교 벤처전문대학원 조교수
〈관심분야〉 정보보호, 유비쿼터스 네트워크 및 보안, 보안 시스템, CERT/CC, Forensic, VoIP 보안, 이동통신 및 WiBro 보안, IT-Convergence