공용 네트워크 구축 장비에서의 포렌식 아티팩트 수집 방안*

이 준 형,[1] 박 상 호[2]
[1]포렌식 인사이트

A Study on Forensic Techniques in public network environments

Jun-Hyeong Lee,[1] Sang-ho Park[2]
[1]Forensic Insight

요 약

최근 스마트기기의 확산으로 다양한 곳에서 공용 네트워크 환경이 설치되어 운용되고 있으며, 이로 인해 공용 네트워크에 접속하고 있는 사용자들의 위험 또한 날이 갈수록 높아지고 있다. 그러나 현재 디지털 포렌식 프로세스는 공용 네트워크 내에서 발생한 침해사고 분석 시 개인 PC를 중점적으로 다룰 뿐 공용 네트워크를 구성하고 있는 장비에 대해서는 관심도가 현격히 적다. 본 논문에서는 공용 네트워크를 구성하고 있는 장비에서 획득 가능한 디지털 포렌식 관점에서의 데이터를 선별하여 정리하고, 정확한 정보를 얻기 위한 방법을 제안한다.

Ⅰ. 서 론

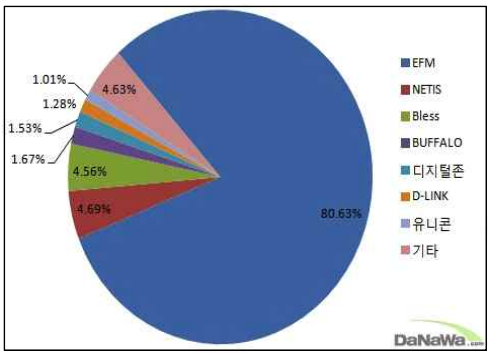
최근 스마트기기의 확산으로 인해 전국적으로 공용 네트워크가 구축, 운용되어 사용자들은 언제 어디서든지 데이터 요금을 지불하지 않고 무료로 인터넷 망을 사용 할 수 있게 되었다. 또한 사내에서도 공용 네트워크 구축 장비(이하 공유기)를 이용한 공용 네트워크 환경을 통해 직원들에게 편리함을 제공하고 있다, 공격자들은 이러한 점을 놓치지 않고 공격의 대상으로 삼고 있으며, 이로 인해 공용 네트워크 사용자들의 보안 위험도가 높아지는 것이 현재의 추세이다. 공격자들은 공용 네트워크의 익명성과 일회적인 위치, 유선 네트워크보다 상대적으로 낮은 보안성을 이유로 이를 공격 대상으로 삼아 침해사고를 일으킨다. 그러나 현재 디지털 포렌식 분야에서는 공용 네트워크 환경에서 침해사고가 일어나더라도 침해사고가 일어난 개인 PC를 중점적으로 사고조사를 할 뿐, 현재 네트워크를 구성하고 있는 장비에 대해서는 큰 관심을 두지 않는다. 본 논문에서는 공유기의 포렌식 가이드라인을 제시 해 보다 정확한 침해사고의 재구성을 꾀하고 개인 PC 흔적과 공유기의 흔적의 논리적인 관계 입증으로 수사에 도움이 되는 연구를 설명하고자 한다.

Ⅱ. 관련 연구

현재 국내에는 많은 공유기 판매 업체들이 존재하며, 각 업체는 각자의 기술과 관리 인터페이스를 사

* 본 연구는 디지털 포렌식 기술 워크샵 제출 논문으로 수행하였습니다.

용자들에게 제공하고 있어 각 공유기에서 획득 할 수 있는 흔적(이하 아티팩트)들은 매우 다양하다. 그러나 국내 공유기 점유율 현황을 살펴보면 EFM社의 아이피타임 공유기가 약 80%로 국내시장에서 매우 높은 점유율을 보이고 있다. 아래 〔그림 1〕은 2013년 국내 공유기 점유율 브랜드별 현황을 나타낸다.



〔그림 1〕 2013년 국내 공유기 점유율 브랜드별 현황(출처 : 다나와 리서치)

위 〔그림 1〕을 통해 대부분의 장소에 구축된 공용 네트워크는 4/5확률로 EFM社의 아이피타임 공유기라고 예상할 수 있다.

현재 우리나라에서는 경찰청에서 발간한 디지털증거 처리 표준 가이드라인에서 네트워크 장비에서 증거를 수집 할 때 준수해야 하는 프로세스와 분석 방법을 대략적으로 설명 해 놓았을 뿐, 자세한 네트워크 장비의 언급과 수집 방법, 분석 방법을 언급하지 않아 디지털 포렌식을 수행하는 인원들에게 오히려 혼란을 초래하고 있다. 이외에 공유기와 같은 공용 네트워크 환경의 디지털 포렌식 기법이 연구되고 있지 않으며, 해외의 경우 라우터를 대상으로 한 네트워크 장비의 포렌식 연구가 선행되었다. 대표적으로 Australian Digital Forensics Conference에서 ADSL 라우터의 라이브 정보 수집 방안, ADSL 라우터의 메모리 덤프 방안, 비활성 정보 수집 및 분석 방안 등에 대한 연구 결과를 제시했으며, Dale Liu는 자신의 저서인 Cisco Router and Switch Forensics: Investigating and Analyzing Malicious Network Activity에서 가장 많이 사용되는 시스코 라우터에 대한 포렌식 방안을 제시하였다. 이는 공유기 포렌식 시에도 많은 도움이 되는 기초 자료 이다.〔1〕〔2〕〔3〕〔4〕〔6〕

Ⅲ. 공유기 포렌식 가이드라인

3.1 국내 공유기 관리 인터페이스

국내 공유기는 공용 네트워크 환경 제어를 위한 관리자 인터페이스를 매우 훌륭히 제공한다. 본 논문에서 다룰 공유기인 아이피타임과 애니게이트 공유기는 인터페이스의 구성에는 차이가 존재하지만, 포렌식 분석 시 수집해야 할 아티팩트 정보들은 대부분 동일하다. 아래 〔표 1〕은 아이피타임의 인터페이스에서 수집해야 할 정보를 수집 가능한 페이지 별로 정리한 표이며, 〔표 2〕는 애니게이트의 인터페이스에서 수집해야 할 정보를 수집 가능한 페이지 별로 정리한 표이다.

〔표 1〕 아이피타임 인터페이스에서의 수집 정보 정리

수집 아티팩트	아티팩트 페이지
DHCP 할당 정보	timepro.cgi?tmenu=netconf&smenu=laninfo
무선 패킷 전송량 정보	timepro.cgi?tmenu=wirelessconf&smenu=info
포트 포워딩 정보	timepro.cgi?tmenu=natrouterconf&smenu=portforward
라우팅 테이블 정보	timepro.cgi?tmenu=natrouterconf&smenu=router
컨넥션 정보	timepro.cgi?tmenu=trafficconf&smenu=conninfo
컨넥션 제어 정보	timepro.cgi?tmenu=trafficconf&smenu=connctrl
시스템 로그 정보	timepro.cgi?tmenu=sysconf&smenu=syslog
타임서버 정보	timepro.cgi?tmenu=sysconf&smenu=realtime

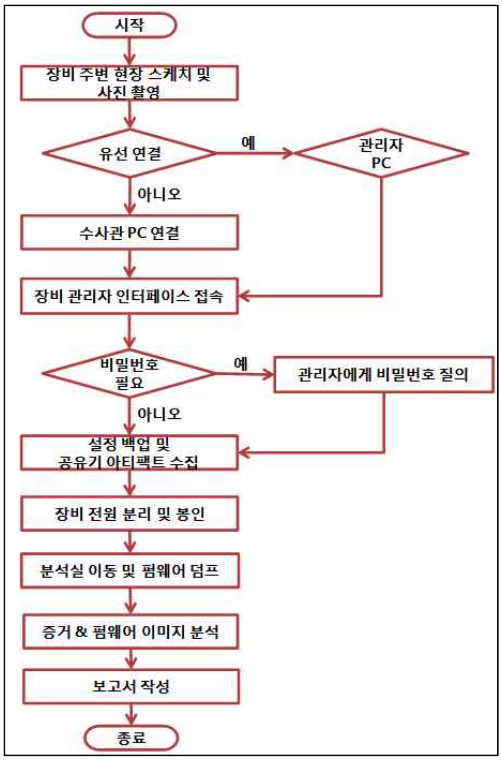
〔표 2〕 애니게이트 인터페이스에서의 수집 정보 관리

수집 아티팩트	아티팩트 페이지
DNS 정보	wan_dynamic.asp
DHCP 사용여부 및 정보	lan_setup.asp
무선 출력 세기 정보	wlan_setup.asp
포트 포워딩 정보	port_forward.asp
아이피 포워딩 정보	ip_forward.asp
사설 아이피 정보	vip_fwd.asp
타임서버 정보	time.asp
라우팅 테이블 정보	ip_route.asp

세부 상태 정보	status.asp
DHCP 할당 정보	dhcp_status.asp
시스템 로그 정보	log.asp

3.2 공유기 포렌식 프로세스

공유기 포렌식은 장비의 특성 상 기존 디지털 포렌식 프로세스와는 조금 다른 프로세스를 가진다. 다음 〔그림 2〕는 공유기 포렌식의 증거 수집 및 분석 과정 프로세스 흐름도이다.



〔그림 2〕 공유기 포렌식 프로세스 흐름도

현장에 도착 시 일반 디지털 포렌식 프로세스와 동일하게 현장 스케치 및 사진 촬영을 수행하며, 현장 스케치에서 유선의 연결 여부를 확인하고 관리자 PC와 유선 연결되어 있다면 아티팩트 수집을 수사관 PC를 사용하지 않고, 이미 연결되어 있는 관리자 PC를 이용하도록 제시하고 있다. 이는 공유기의 기억장치 용량이 일반 시스템 기억 장치 용량과는 다르게 소규모이기 때문에, 장비를 연결할 경우 해당 장비의 연결만으로도 수사관에게 필요한 여러 정보들이 로그 생성 및 프로세스 수행으로 인해 사라질 수 있기 때문이다. 만약 유선으로 연결되어 있는 PC가 없다면 수사관의 PC를 연결하며, 해당 공유기의 관리 인터페이스로 접속을 시도 한다. 관리 인터페이스에 비밀번호가 설정되어 있을 시에는 관리자에게 비밀번호를 요청하고, 비밀번호가 존재하지 않는다면 바로 관리자 인터페이스 접속 후 이미 설정되어 있는 여러 설정들을 백업을 통해 수집한다. 그 후 본 논문에서 제시하는 여러 아티팩트들을 수집하며, 장비의 전원을 장비 본체와 분리 한 후 봉인 및 분석실로 이동하여 공유기의 펌웨어 덤프를 수행한다. 덤프를 수행한 펌웨어 이미지를 분석 해 복구 할 수 있는 내용이 있는지, 공유기 웹 서버의 불법적인 침입은 없었는지 등을 살핀 후 보고서를 작성하여 제출하는 것으로 공유기 포렌식 프로세스를 끝마친다.

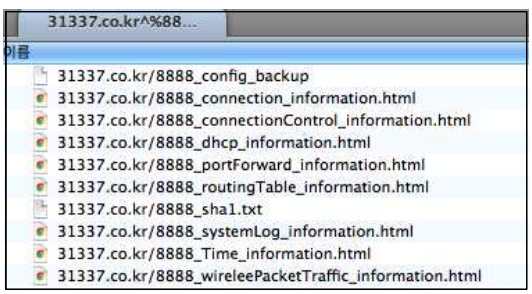
3.3 아티팩트 수집 도구 설계

국내 공유기 업체들은 각 업체별로 고유한 구조와 관리자 인터페이스를 사용자들에게 제공하고 있으며, 출시 모델에 따라 사양이 다양하여 아티팩트 수집 시 해당 모델의 업체뿐만 아니라 사양 또한 고려해야 한다. 공유기에서 생성하는 정보 중 포렌식 적으로 가장 의미있는 정보는 '공유기 시스템 로그'이다. 공유기 시스템 로그는 공유기가 가지는 하드웨어 사양에 따라 생성 및 삭제 시점이 달라지며, 모델에 따라 저장하는 방식도 다르다. 본 논문에서 언급하는 아이피타임 공유기의 경우 DRAM 사양이 16MB ~ 64MB 이고 FLASH 사양이 4MB ~ 16MB 이다. 애니게이트의 경우 DRAM 사양이 16MB ~ 64MB이고, FLASH 사양이 2MB ~ 4MB 이다. 애니게이트의 경우 FLASH 용량이 매우 작기 때문에 기본적으로 시스템 로그를 공유기 자체에 생성하는 것 외에 외부서버에 생성하는 방식도 지원하고 있다. 이와 같이 공유기 포렌식을 수행 할 시에는 아티팩트 수집과 동시에 데이터 생성 장소 설정 등에 대한 분석또한 현장에서 이루어져야 다음 조치를 신속하게 취할 수 있다.

본 논문에서 제시하는 수집 도구는 아이피타임과 애니게이트 아티팩트 수집 도구로 나뉜다. 공통적으로 웹 페이지 크롤링을 수행하며, 이는 아티팩트 정보를 포함한 페이지를 크롤링하여 저장하고, 저장 된 페이지의 해시 값을 계산하여 텍스트 파일로 저장한다. 설정 백업 파일 역시 크롤링을 수행함으로서 수

집 가능하다. 아이피타임 아티팩트 수집 도구의 경우 아이피타임 페이지가 하나의 cgi 파일에서 파라미터 값을 이용 해 페이지를 구분하기 때문에 파라미터 값의 변화를 주어 페이지를 수집 하고, 애니게이트 수집 도구의 경우 아티팩트를 포함하고 있는 페이지가 모두 asp로 개별적으로 존재하기 때문에 각 페이지에 대한 요청을 수행 하여 수집 한다. 아래 〔그림 3〕은 아티팩트 수집 도구의 진행 출력의 일부이며, 〔그림 4〕는 아티팩트 수집 도구가 수집한 페이지들의 결과 화면이다. 실제 수집 도구에서는 zip파일 결과를 제공한다.

〔그림 3〕 수집 도구 진행 출력의 일부



〔그림 4〕 수집 결과물

Ⅳ. 공유기 분석 사례

공용 네트워크 침해사고에 따른 공유기 포렌식 수행은 크게 두 가지로 나눌 수 있다. 첫 번째는 '다른 네트워크 또는 호스트의 침해사고 경로가 된 경우'이며, 두 번째는 '연결된 호스트 또는 네트워크 자체가 침해 사고를 당한 경우' 이다.

4.1 공유기가 다른 침해사고의 경로가 된 경우

이 경우 용의자는 자신의 물리적 위치를 숨기기 위한 목적일 가능성이 가장 크며, 만약 용의자가 특정 장소에서 침해사고를 일으켰다는 것을 논리적으로 입증해야 한다면, 아래 〔그림 5〕와 같이 공유기의 시스템 로그를 분석해 DHCP 할당 정보와 용의자 PC의 DHCP 할당 정보를 수집하여 두 아티팩트 간의 관계를 통해 분석 시 도움이 될 수 있다.

2013/08/13 22:17:47	DHCP 서버가 IP 할당함: 192.168.0.7
2013/08/13 22:08:18	DHCP 서버가 IP 할당함: 192.168.0.126
2013/08/12 21:18:34	DHCP 서버가 IP 할당함: 192.168.0.7
2013/08/11 18:59:57	DHCP 서버가 IP 할당함: 192.168.0.7
2013/08/11 15:32:48	DHCP 서버가 IP 할당함: 192.168.0.72
2013/08/11 15:19:56	DHCP 서버가 IP 할당함: 192.168.0.77
2013/08/10 14:11:37	DHCP 서버가 IP 할당함: 192.168.0.69
2013/08/10 09:21:05	DHCP 서버가 IP 할당함: 192.168.0.72
2013/08/09 23:39:51	DHCP 서버가 IP 할당함: 192.168.0.117
2013/08/09 20:22:05	DHCP 서버가 IP 할당함: 192.168.0.77

〔그림 5〕 아이피타임 시스템 로그

대표적으로 윈도우 운영체제에서 DHCP 할당 정보를 획득할 경우 윈도우 운영체제 7을 기준으로 아래 〔표 3〕의 레지스트리 경로에서 해당 정보를 획득할 수 있다.〔5〕

〔표 3〕 무선 네트워크 정보 획득 레지스트리 경로

정보 분류	경로
접속 공유기 및 시간 정보	HKLM\Software\Microsoft\Windows NT\NetworkList\Nla〈Wireless, Signature, Profile〉
DHCP 할당 정보	HKLM\System\CurrentControlSet\Service\Tcpip\Parameters\Interface\〈NIC GUID〉

〔표 3〕의 레지스트리 분석을 통해 접속한 공유기의 이름, 접속 시간, 접속 공유기의 고유 값, 할당 받은 사설 아이피 또는 사용자가 수동으로 설정한 아이피 등을 획득 할 수 있으며, 이를 통해 특정 시간에 특정 공유기에 접속하였다는 것을 확인할 수 있다. 또한, 물리적인 위치를 추적하기 위해서는 공유기의 무선 출력 세기를 측정 해 공유기 주위로부터 몇 m이내에서 공유기에 접속이 가능한지를 파악 해 주위 CCTV를 획득 및 분석하면 용의자가 어느 장소에서 공유기에 접속 했는지 파악 할 수 있다.

4.2 공유기 네트워크 자체가 침해 된 경우

이 경우 용의자는 공유기 네트워크에 접속한 사용자들의 개인정보를 탈취하기 위한 목적일 가능성이 가장 크며, 용의자 입장에서 가장 쉽게 개인정보를 탈취 할 수 있는 방법은 'MITM(Man In The Middle)' 공격이기 때문에, 용의자는 공유기의 관리자 인터페이스에서 제공하는 있는 라우팅 테이블 또는 포워딩 기능을 이용 해 모든 호스트의 패킷이 자신을 거쳐 가게끔 하는 공격을 할 가능성이 높다. MITM 공격 수행 전 만약 관리자 인터페이스에 비밀번호가 설정되어 있다면 용의자는 공유기 자체의 취약점 또는 무작위 대입 공격을 통해 비밀번호를 획득할 가능성이 높다. 이 때 모든 접근 시도는 로그 파일로 기록되며, 용의자가 공유기 관리자 인터페이스에 어떻게 접근 했는지 파악 할 수 있다. MITM 공격을 시작하면, 공유기를 통한 모든 패킷은 용의자 PC에 구축되어 있는 프록시 서버로 인해 모두 복호화 되어 개인정보가 유출될 가능성이 있다. 만약 이런 상황을 일반 사용자들이 접한다면 자신의 개인정보가 유출되었다는 것을 판단하기 힘들며, 수사관이 개인 사용자의 PC를 분석하여도 해킹 침해에 대한 증거를 획득하기 어렵다. 이럴 경우 공유기 포렌식을 수행하여 공유기에 설정되어 있는 현재 설정을 분석하는 것이 가장 바람직하다. 아래 〔그림 6〕은 공유기(192.168.10.1)로 도착하는 패킷이 모두 공격자(192.168.10.7)에게 돌아가도록 설정한 정적 라우팅 테이블 모습이다.

〔그림 6〕 애니게이트 정적 라우팅 테이블

분석을 위해서는 공유기 관리자 인터페이스에서 라우팅 테이블, 포트 포워딩 등의 설정과 용의자 PC를 분석하여 동일시간에 두 무선 네트워크에 접속한 흔적을 획득해야 한다. 공유기의 관리자 인터페이스에서 패킷의 흐름을 바꾸는 설정을 할 경우 용의자는 자신에게 온 패킷이 모두 정상적으로 인터넷 통신이 될 수 있도록 전달해야 하며, 해당 공유기를 이용해서는 인터넷 통신을 할 수 없기 때문에 용의자는 자신의 PC에 추가로 네트워크 카드를 장착하고 주변에 존재하는 공유기에 접속하여 해당 공유기로 모든 패킷을 포워딩 하거나, 휴대용 무선 공유기를 이용해 패킷들을 인터넷으로 포워딩해야 한다. 이 모든 행동은 동시간대에 일어나는 행동이므로 용의자 PC에서 이와 같은 흔적을 발견한다면 용의자 선별이 쉬워진다.

Ⅴ. 결 론

네트워크의 발전과 확산에 따라 네트워크 침해사고가 많이 발생함에도 불구하고 현재 네트워크 포렌식에 대한 연구가 굉장히 미흡하다. 본 논문에서는 이러한 국내의 현실을 되짚어보고 발전을 도모하고자 공용 네트워크를 구축하는데 가장 많이 사용되는 공유기에 대한 포렌식 연구를 진행하였다. 우리나라에 특화된 공유기 포렌식을 연구하고 수사에 적용함으로써 사건의 재구성과 정확한 범죄사실, 범죄방법 등을 알아 낼 수 있었으며 앞으로 공유기 포렌식의 흔적 수집과 분석을 모두 지원하는 자동화 도구를 개발한다면 수사의 편의성과 효율성을 증대 시킬 수 있을 것이라 생각 된다.

참 고 문 헌

[1] Patryk Szewczyk, "ADSL Router Forensics Part 1: An introduction to a new source of electronic evidence," 5th, Australian Digital Forensics Conference, 2007년 12월.

[2] Patryk Szewczyk, "ADSL Router Forensics Part 2: Acquiring Evidence," 7th Australian Digital Forensics Conference, 2009년 12월.

[3] Patryk Szewczyk, "The ADSL Router Forensics Process," 2ECU Publications Pre. 2011, Journal of Network Forensics, 2(1), 4-13, 2010년.

[4] Dale Liu, "*Cisco Router and Switch*

Forensics: Investigating and Analyzing Malicious Network Activity" 2009년 4월.

[5] 이준형, 조정원 "*디지털 포렌식의 세계*", 인포더북스, 2013년 2월

[6] 경찰청, "디지털증거 처리 표준 가이드라인" (사)한국디지털포렌식학회, 2006년 12월