제10장 윈도우 시스템 조사

박 종 혁 교수

UCS Lab

Tel: 02-970-6702

Email: jhpark1@seoultech.ac.kr

개요

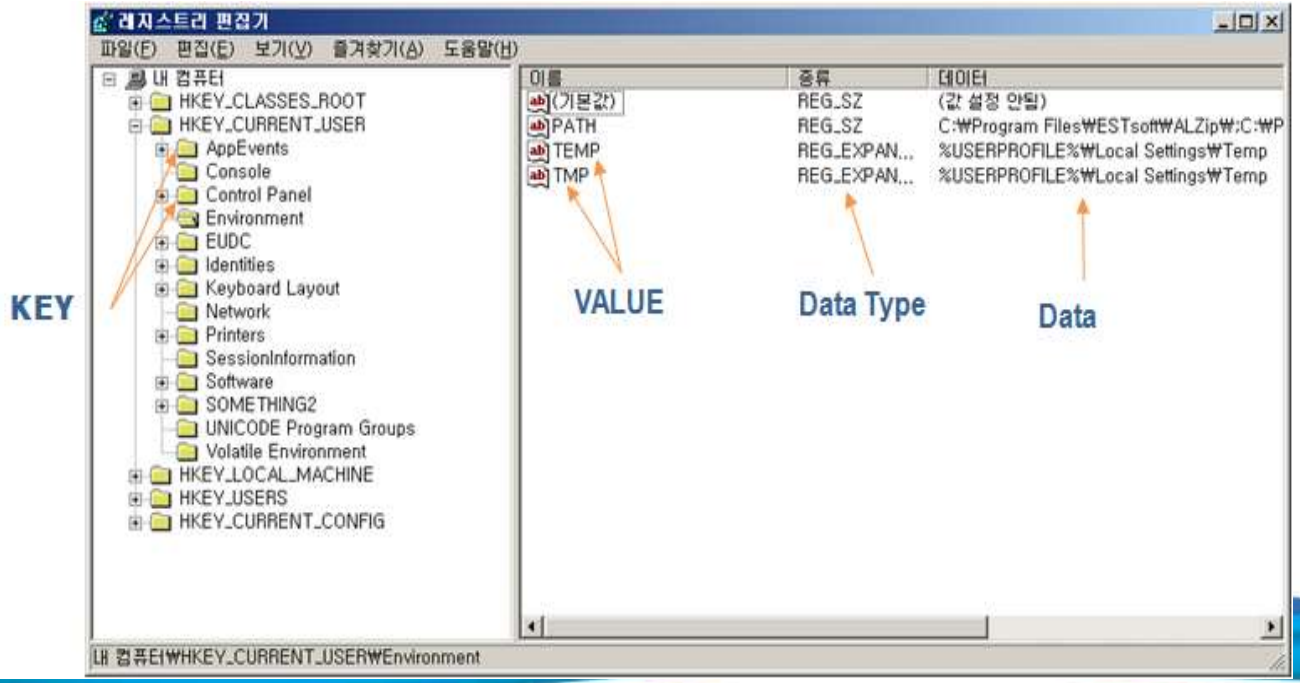
- 학습목표
  - 윈도우 시스템의 휘발성 데이터, 환경 설정에 관련된 레지스트리, 네트워크 설정 및 사용현황에 관한 정보, 인터넷 서핑 기록을 알 수 있는 웹브라우저, 인터넷 메신저의 정보 수집에 대해 학습한다.

- 학습 내용
  - 윈도우 레지스트리
  - 네트워크 정보
  - 웹브라우저
  - 인터넷 메신저

목 차

윈도우 레지스트리

- 레지스트리 소개
  - 레지스트리는 마이크로소프트 윈도우 95 이후 버전에서 도입된 환경 설정에 관한 일종의 데이터베이스
  - 운영체제 및 응용 프로그램 운영에 필요한 정보를 저장 및 관리
  - 부팅 과정에서 사용되는 정보, 로그인, 서비스 실행, 응용 프로그램 실행, 사용자 실행 등
  - 파일 시스템의 구성요소와 유사
  - 모든 값(Value)은 키 내에 위치하며, 키들은 계층형 구조



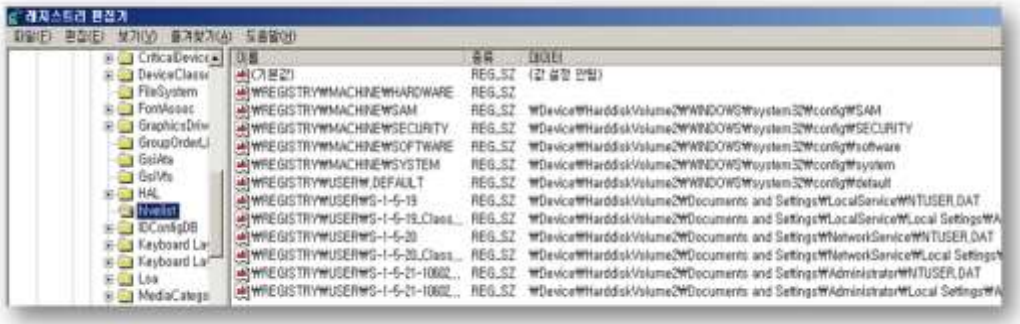
윈도우 레지스트리

- 레지스트리는 디스크 상에서 “하이브(Hive)"로 불리는 분리된 파일로 존재
  - 윈도우 부팅과정에서 메모리에 적재되어 관리
  - 레지스트리 정보를 디스크에 저장한 바이너리 파일
  - 시스템이 로그온 되면 시스템 커널 프로그램에 의해 관리
  - 하이브 파일의 목록

하이브 파일 이름	윈도우레지스트리 경로	저장 정보
HKEY_USER₩.DEFAULT	Default	사용자 계정이 생성될 때, 기본적으로 필요한 정보를 저장한다.
KKEY_LOCAL_MACHINE₩SOFTWARE	Software	응용 프로그램 정보
HKEY_LOCAL_MACHINE₩SAM	Sam	사용자 계정정보 저장
HKEY_LOCAL_MACHINE₩SECURITY	Security	감사정책 및 권한정보 저장
HKEY_LOCAL_MACHINE₩SYSTEM	System	하드웨어 드라이버 및 구성정보
HKEY_USERS	Ntuser.dat(각 계정마다 하나씩 별도)	사용자 계정에 설정된 정보 저장

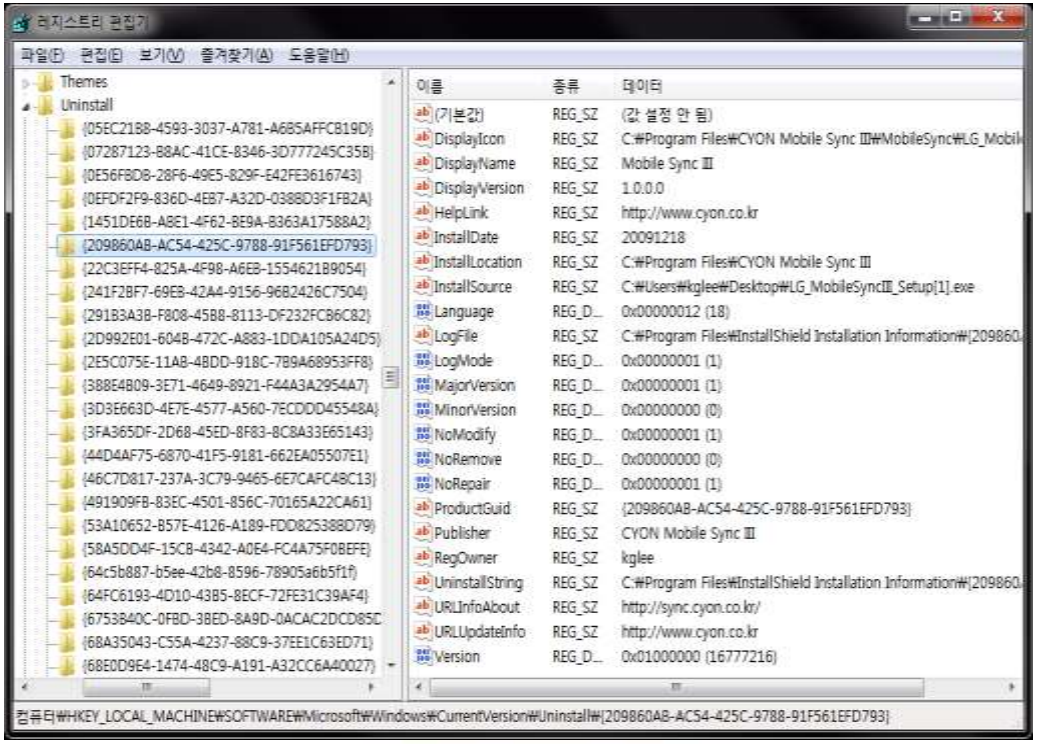
윈도우 레지스트리

- HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentContolSet₩Control₩hivelist 경로에 각각에 해당하는 하이브 파일의 위치 정보가 저장
  - 포렌식 조사를 위해서는 레지스트리의 위치정보를 숙지
- 디지털 포렌식 조사 관점에서 레지스트리는 사용자의 활동 정보나 응용 프로그램 사용 흔적, 설치된 하드웨어 및 소프트웨어 정보, 네트워크 설정 정보와 같은 많은 디지털 증거를 수집할 수 있는 포렌식 자원
  - 각각의 키에 마지막 수정 시각(Last Written Time)이 기록되어 있기 때문에 일종의 로그로써 활용



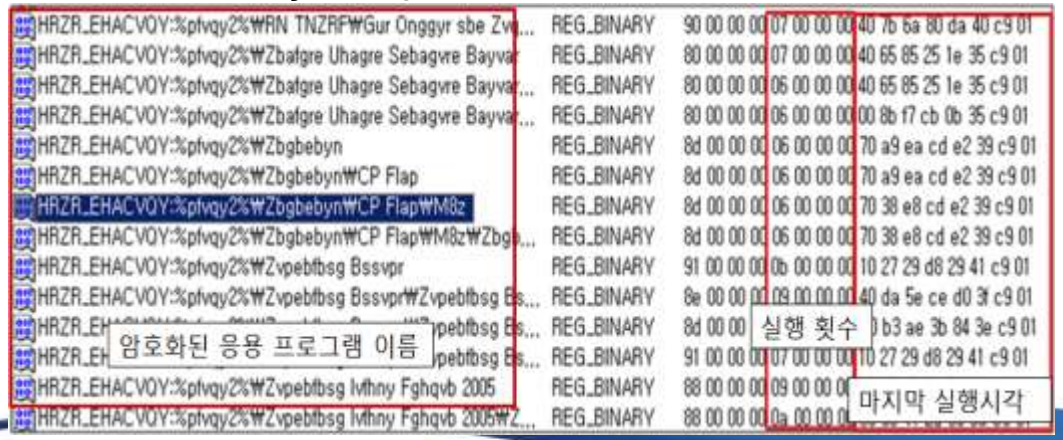
레지스트리 포렌식 분석

- 설치된 프로그램 목록
- HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩UnInstall 경로에 설치된 프로그램의 이름, 버전, 게시자, 설치 시각, 설치 위치, 소스 경로가 저장

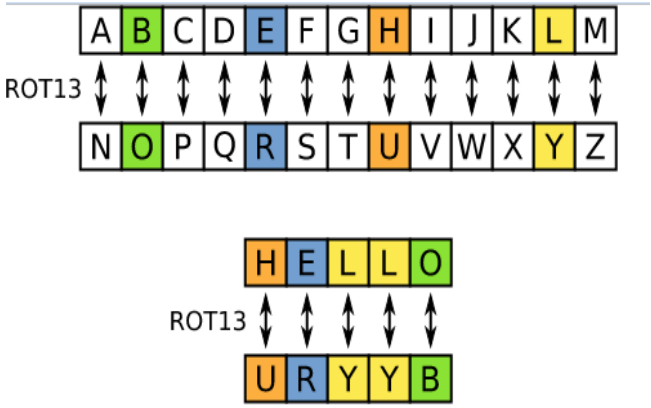


레지스트리 포렌식 분석

- 하위 키는 설치된 응용 프로그램의 목록(SID로 표시)을 가리키고, 값에 설치된 프로그램 정보가 저장
  - 프로그램 추가・삭제 목록을 조사하여 사용자가 의도하지 않은 특정 프로그램이 설치되어 있는지 조사하고, 해당 프로그램이 정상적인 프로그램인지를 확인
- HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist₩{5E6AB780-7743-11CF-A12B-00AA004AE837}₩Count
  - 실행한 프로그램의 경로와 실행 유형, 실행 횟수, 최종 실행 시간이 저장
- 값의 이름이 ROT13(Caesar cipher)으로 암호화
  - ROT13은 Rotate by 13 places의 줄임말로 간단한 치환 암호



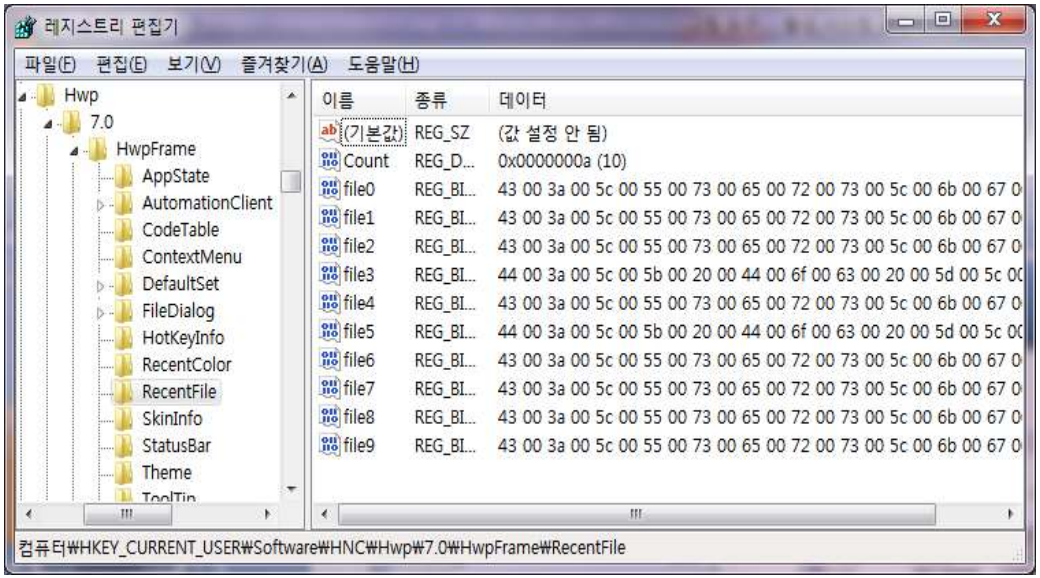
레지스트리 포렌식 분석



- 실행 횟수의 시작값은 5
- 마지막 실행 시각은 FILETIME 형식으로 저장
  - 이 값을 조사하여 의심스러운 시간대에 특정 파일이 실행되었는지 유무를 확인
  - 특히 이 항목들은 악의적인 프로그램을 삭제한 후에도 레지스트리에 남아 있기 때문에 중요한 증거로 사용될 수 있다.

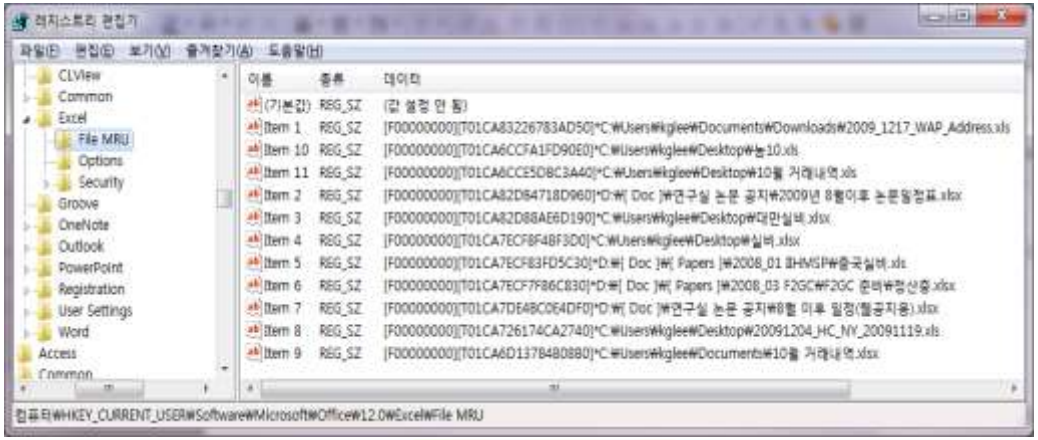
레지스트리 포렌식 분석

- 한글 2007
- HKEY_CURRENT_USER₩Software₩ HNC₩Hwp₩7.0₩HwpFrame₩RecentFile
  - 최근 사용한 문서의 목록이 최대 10개까지 저장



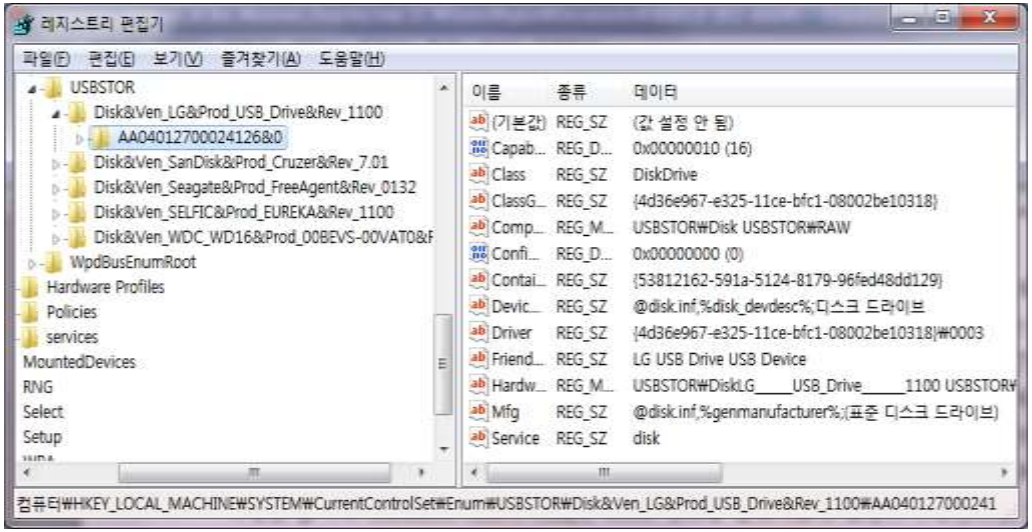
레지스트리 포렌식 분석

- 마이크로소프트 오피스 2007
  - 최근 접근 문서가 최대 50개까지 저장
  - 마이크로소프트 오피스 엑셀, 파워포인트, 워드 프로세스가 모두 동일
  - item 0가 최근에 사용한 문서
  - HKEY_CURRENT_USER₩Software₩Microsoft₩Office₩12.0₩{Excel|PowerPoint|Word}₩File MRU
    - 최근 사용한 문서의 정보가 저장



레지스트리 포렌식 분석

- USB(Universal Serial Bus)에 장치를 연결하면 관련 드라이버 정보 등이 레지스트리에 저장
  - HKEY_LOCAL_MACHINE₩SYSTEM ₩CurrentControlSet₩Enum₩USBSTOR
  - 해당 시스템에 연결된 적이 있는 모든 USB 저장 장치의 생산자와 ID 값 등이 기록

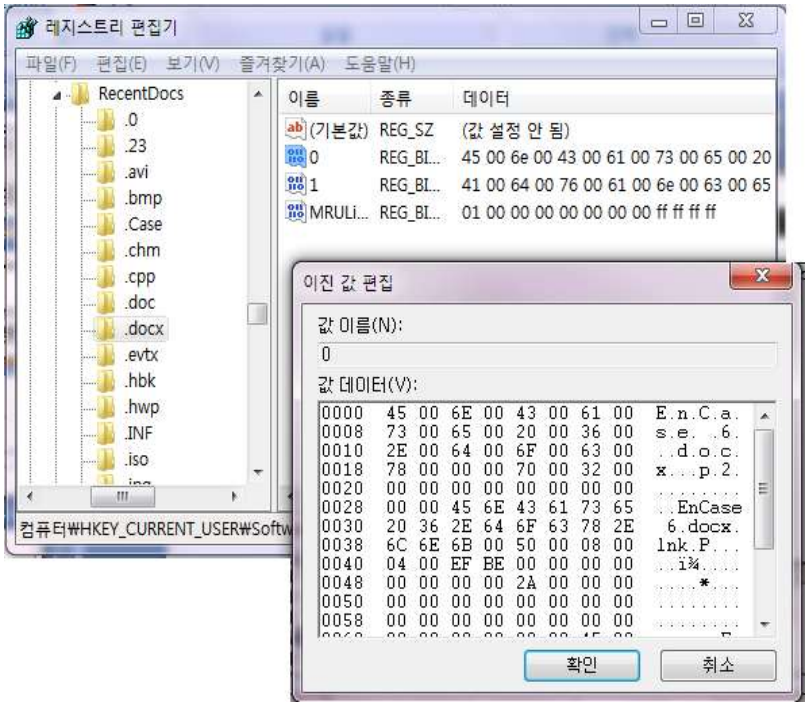


레지스트리 포렌식 분석

- {*Device Type*}&Ven_{*Vendor String*}&Prod_{*Product String*}&Rev_{*Version Information*}
  - Device Type은 해당 장치의 종류
  - Vendor String에는 제조사
  - Product String에는 제품 이름
  - Version Information에는 제품 버전
  - 선택된 키는 해당 장치의 Unique Instance ID
    - 해당 값은 다른 시스템에 연결될 때도 같은 값으로 나타나기 때문에, USB 저장장치를 특정할 수 있다.
    - 일부에 해당 값이 없는 경우가 존재
  - 이 경우 윈도우 시스템의 PnP Manager가 자동으로 Prefix 값을 할당
    - 동일한 USB 저장장치라 할지라도 다른 시스템에 연결될 때, 서로 다른
    - 해당되는 USB 저장장치를 특정할 수는 없다.

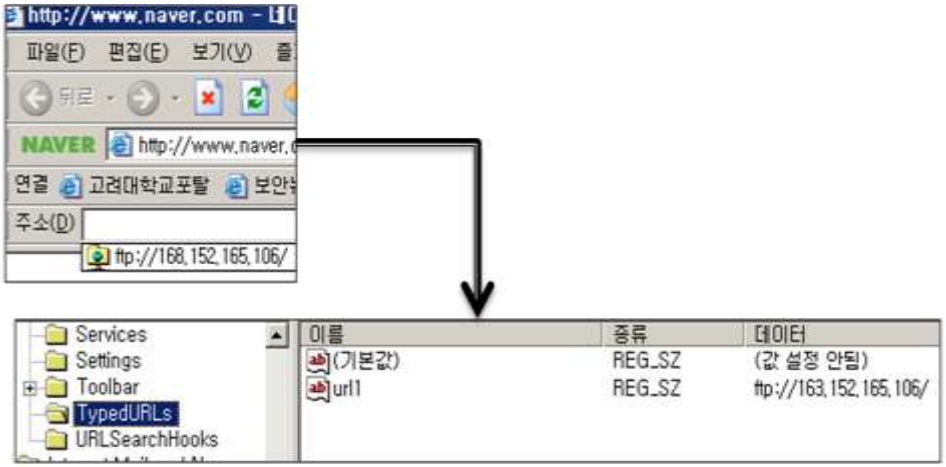
레지스트리 포렌식 분석

- HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion ₩Explorer₩RecentDocs
  - 하위키는 확장자 별로 구분하여 사용된 문서 정보를 저장
  - 해당 값은 유니코드로 저장



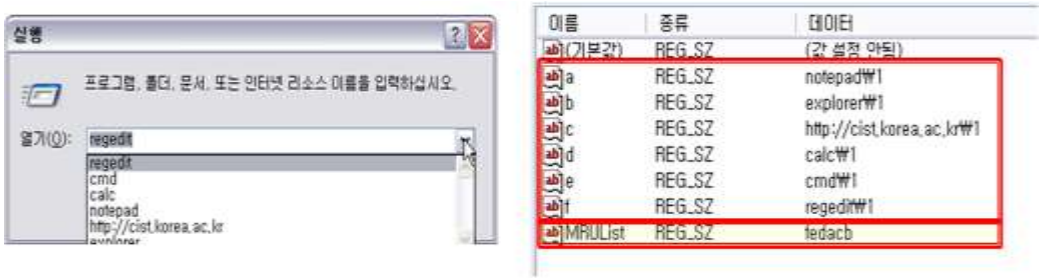
레지스트리 포렌식 분석

- 인터넷 익스플로러(Internet Explorer)
  - 웹 브라우저 주소창에 기록하는 주소 목록
  - HKEY_CURRENT_USER₩Software₩Microsoft₩Internet Explorer₩TypedURLs
    - 사용자가 자주 접속하는 웹 페이지, 주제, 키워드 등을
    - 인터넷 익스플로러 7 버전부터는 해당 경로에 기록하지 않음



레지스트리 포렌식 분석

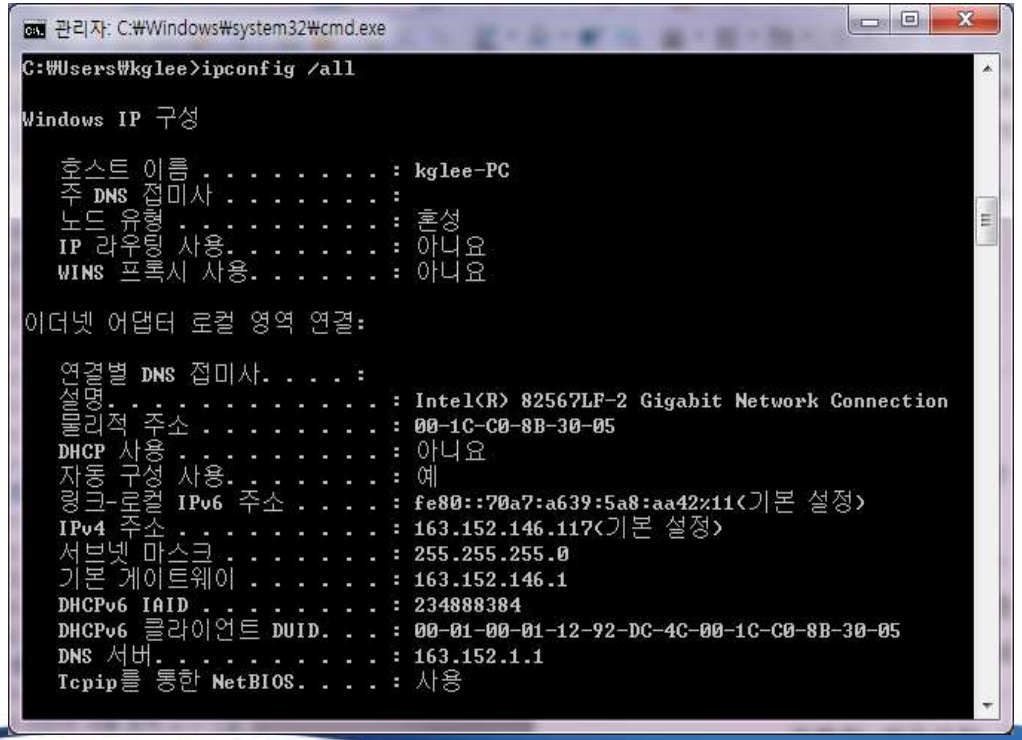
- 윈도우의 실행 창을 통해서 입력된 명령어 목록
  - HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩RunMRU
  - 실행한 순서는 MRUList(Most Recent Used List) 값
    - 이 값은 가장 최근에 사용된 명령어 순서로 값 정보를 저장한 배열



    - b가 가장 먼저 실행되었고, c, a, d, e, f 순서로 실행되었음을 의미

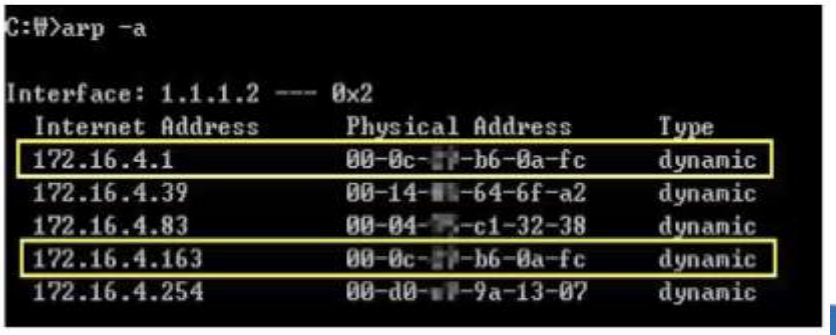
네트워크 정보

- 네트워크 장치는 주로 사용되는 이더넷(Ethernet) 카드, IEEE 802.11x를 지원하는 무선 접속 단말기 등을 의미
- 해당 시스템에 연결된 모든 네트워크 장치에 할당된 IP 정보, MAC 주소, 하드웨어 ID 등을 조사하여 어떤 주소로 통신을 송수신했는지 파악할 필요이 정보를 활용하여 추후 침입 탐지 사례를 조사할 경우, 보다 정확한 재구성 가능



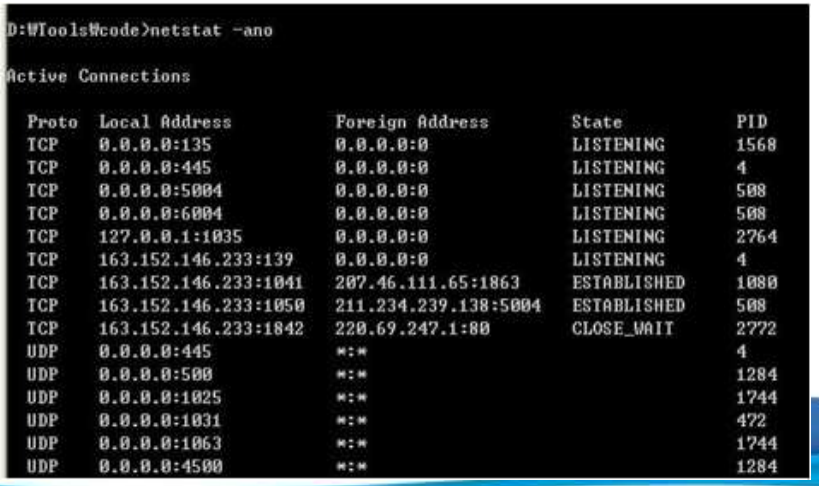
네트워크 정보

- 네트워크 테이블
  - 라우팅(Routing) 테이블 : IP정보를 저장
  - ARP(Address Resolution Protocol) 테이블 : MAC 주소를 저장
- ARP 스푸핑(Spoofing) 공격
  - 대상 시스템의 ARP 테이블을 변조하여 게이트웨이의 MAC 주소와 공격자의 MAC 주소를 동일하게 설정
  - 대상 시스템에서 전송되는 모든 패킷은 공격자의 시스템으로 동일하게 전송되며, 공격자는 대상 시스템의 모든 패킷을 모니터링
  - 네트워크 테이블을 조사하여 비인가된 주소를 가지고 있는 항목이 없는지를 확인
  - 특정 MAC 주소가 서로 다른 IP에서 나타날 경우, ARP Spoofing을 의심



네트워크 정보

- 악성 프로그램은 대상 시스템의 네트워크 포트를 열어 공격자와 통신
- 공격자는 시스템을 장악하고 나서 이후에 다시 대상 시스템에 쉽게 접근하기 위해 백도어(Backdoor)를 설치, 연결
- 현재 네트워크 연결 상태를 확인하고 사용 정보를 바탕으로 비인가된 접속을 판별
  - 외부와 연결된 포트를 확인
  - 해당 포트를 사용하는 프로세스를 판별 같이 호스트로 들어온 연결 정보, 호스트에서 나가는 연결 정보를 통해서 침입 흔적을 발견할 수 있다.



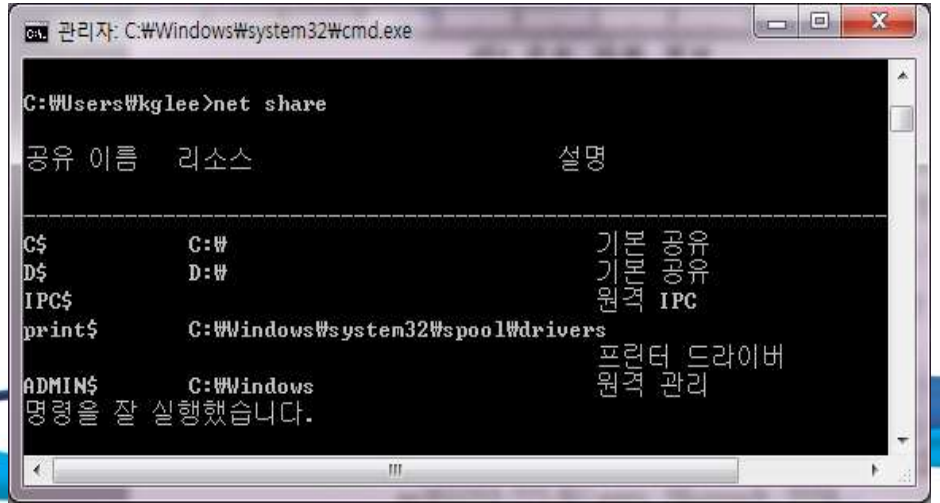
```
D:\Tools\code>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1568
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5004           0.0.0.0:0              LISTENING       508
  TCP    0.0.0.0:6004           0.0.0.0:0              LISTENING       508
  TCP    127.0.0.1:1035         0.0.0.0:0              LISTENING       2764
  TCP    163.152.146.233:139    0.0.0.0:0              LISTENING       4
  TCP    163.152.146.233:1041   207.46.111.65:1863     ESTABLISHED     1080
  TCP    163.152.146.233:1050   211.234.239.138:5004   ESTABLISHED     508
  TCP    163.152.146.233:1842   220.69.247.1:80        CLOSE_WAIT      2772
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    1284
  UDP    0.0.0.0:1025           *:*                                    1744
  UDP    0.0.0.0:1031           *:*                                    472
  UDP    0.0.0.0:1063           *:*                                    1744
  UDP    0.0.0.0:4500           *:*                                    1284
```

네트워크 정보

- SMB(Server Message Block) 프로토콜
  - 동일 도메인 내의 시스템 사이의 자원을 공유
  - CIFS(Common Internet File System)
  - OSI 7 계층 중 애플리케이션 레벨에서 동작
  - 파일, 프린터와 같은 다양한 네트워크 공유 지원
  - NET SHARE : 현재 시스템에서 열린 공유 자원의 정보
  - NET SESSION : 원격으로 시스템에 접근하여 사용되고 있는 자원
  - NET FILE : 원격 사용 파일, 전체 경로 및 원격으로 접속한 사용자의 ID를 출력
  - SMB 프로토콜의 취약점을 이용하여 원격에서 코드를 실행



웹브라우저 – Internet Explorer

- Internet Explorer
  - Temporary Internet File : 웹 서버로부터 불러온 임시 파일을 저장
  - Cookies : 쿠키 파일
  - History : 사용자가 접속한 웹 사이트의 목록을 저장
    - 모두 index.dat 파일을 통하여 관련 정보를 관리
  - 운영 체제 버전에 따른 index.dat 파일의 저장 위치

운영 체제	저장 위치
윈도우 95/98/Me	·₩WINDOWS₩Temporary Internet Files₩Content.IE5 ·₩WINDOWS₩Cookies ·₩WINDOWS₩History₩History.IE5
윈도우 NT	·₩Winnt₩Profiles₩<username>₩Local Setting₩Temporary Internet Files₩Content.IE5 ·₩Winnt₩Profiles₩<username>₩Cookies ·₩Winnt₩Profiles₩<username>₩Local Setting₩History₩History.IE5
윈도우 2K/XP	·Documents and Settings₩<username>₩Local Settings₩Temporary Internet Files₩Content.IE5₩ ·Documents and Settings₩<username>₩Cookies₩ ·Document and Settings₩<username>₩Local Settings₩History₩History.IE5₩
윈도우 Vista	·Users₩<username>₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.IE5 ·Users₩<username>₩AppData₩Local₩Microsoft₩Windows₩History₩History.IE5 ·Users₩<username>₩AppData₩Roaming₩Microsoft₩Windows₩Cookies

웹브라우저 – Internet Explorer

- History – index.dat
  - 접속한 url, 다운로드 받은 파일, 마지막 방문 시간을 확인
  - 검색어를 추출 : 검색 사이트마다 쿼리 내용과 인코딩 방법을 분석
  - Ex) (1) (2) (3)
    http://search.naver.com/search.naver?where=nexearch&query=%BC%AD%BF%EF%B
    B%EA%BE%F7%B4%EB&x=42&y=23&sm=top_hty&fbm=1

검색 사이트	페이지 (1)	쿼리 변수(2)	인코딩 방법(3)
Naver	search.naver.com/search.naver	query	멀티바이트, UTF-8
Google	google.co.kr/search	q	UTF-8
Daum	search.daum.net/search	q	멀티바이트
Yahoo	search.yahoo.com/search	p	멀티바이트
Empas	search.empas.com/search	q	멀티바이트

- Activity Record의 url을 통해 다운로드 받은 파일을 확인
  - ex) file:///c:/abcd.txt

웹브라우저 – Internet Explorer

- Temporary Internet File – index.dat
  - 저장된 임시 파일의 url, 임시파일의 저장위치, 임시파일의 이름, 접속 시간을 확인
  - "directory 인덱스"와 "파일 이름 오프셋"을 이용하여 directory 이름과 임시 파일 이름을 확인하면 해당 웹 메일이 어느 위치에 저장되었는지 쉽게 알 수 있다. 쿠키 파일

- Cookies – index.dat
  - Cookies를 저장하는 사이트의 URL, 생성 시간, 최근 접근 시간, 정보를 저장하는 쿠키 파일의 이름을 확인

웹브라우저 – FireFox

- FireFox
  - 임시 파일, 웹 히스토리, 쿠키를 저장
  - FireFox3와 FireFox2 사용 정보를 저장하는 방법이 다름
  - 버전 2에서 버전 3로 업데이트 하더라도 버전 2를 사용하였을 때의 로그가 대상 시스템에 남아 있을 가능성이 있다.

	FireFox2	FireFox3
임시파일	Cache	Cache
웹 히스토리	history.dat	places.sqlite,
쿠키	cookies.txt	cookies.sqlite

웹브라우저 – FireFox

- FireFox 버전별 파일 저장 위치(WinXp의 예)

버전	저장 위치
FireFox2	· Documents and Settings₩<username>₩Local Settings₩Application Data₩Mozilla₩Firefox₩Profiles₩<Random Text>₩Cache · Documents and Settings₩<username>₩Application Data₩Mozil la₩Firefox₩Profiles₩<Random Text>₩history.dat · Documents and Settings₩<username>₩Application Data₩Mozill a₩Firefox₩Profiles₩<Random Text>₩cookies.txt
FireFox3	· Documents and Settings₩<username>₩Local Settings₩Application Data₩Mozilla₩Firefox₩Profiles₩<Random Text>₩Cache · Documents and Settings₩<username>₩Application Data₩Mozil la₩Firefox₩Profiles₩<Random Text>₩places.sqlite · Documents and Settings₩<username>₩Application Data₩Mozill a₩Firefox₩Profiles₩<Random Text>₩cookies.sqlite

웹브라우저 – FireFox

- places.sqlite, cookies.sqlite
  - 웹 히스토리를 저장
  - SQLite database : 임베디드 데이터베이스 라이브러리, 하나의 라이브러리에 데이터베이스 인터페이스를 병합한 형태이다.
  - Places.sqlite : 웹 히스토리를 저장
  - cookies.sqlite : 쿠키를 저장한다.
- cookies.sqlite
  - 쿠키를 저장
  - moz_cookies라는 한 개의 테이블이 존재
  - 호스트 이름, 폐기 날짜, 값, 값의 이름, 마지막 접근 시간 등의 정보

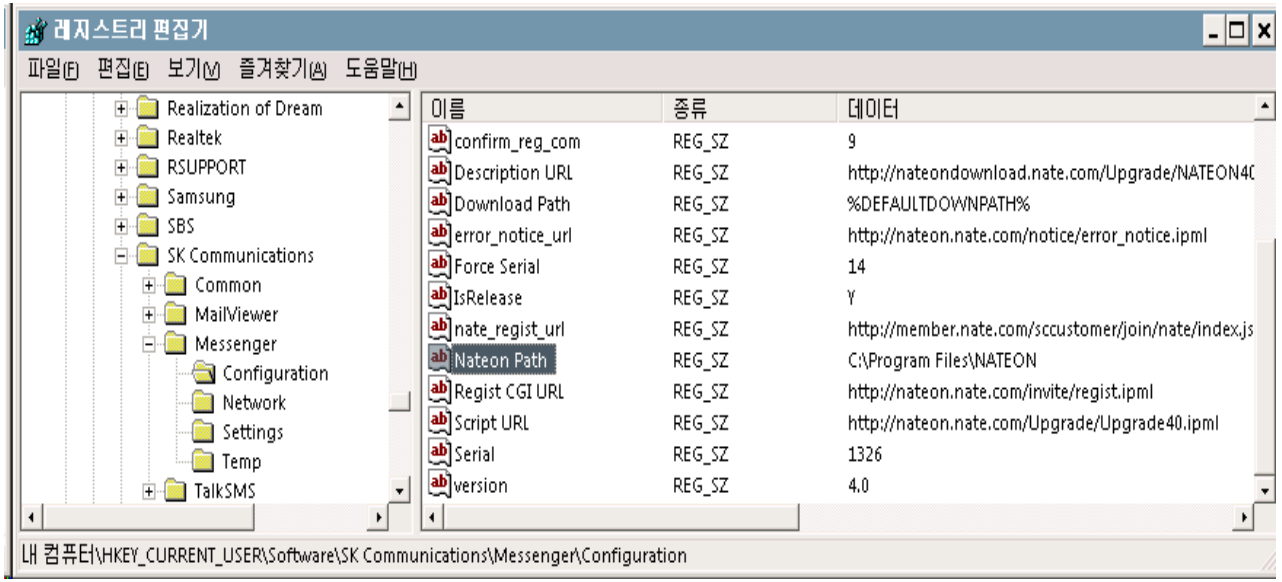
웹브라우저 – FireFox

- places.sqlite – moz_places, moz_historyvisits 테이블
  - moz_places 테이블
    - 방문한 웹 사이트의 url과 해당 웹 페이지 제목, 방문한 횟수, 주소를 직접 입력하여 접속하였는지 여부 등의 정보를 제공
  - moz_historyvisits
    - 사용자가 해당 웹 사이트를 방문한 시간 정보 visit_date
    - moz_places 테이블의 id와 moz_historyvisits 테이블의 places_id를 결합하면 사용자가 해당 url에 접속하였을 때의 시간 정보를 알 수 있다.

테이블	항목	설명
moz_places	id	각 record마다 주어지는 고유 번호
	url	사용자가 접속한 url
	title	해당 웹 페이지 제목
	rev_host	호스트 이름을 역순으로 나열한 것
	visit_count	방문한 횟수
	typed	사용자가 주소를 직접 입력 하였는지 여부
	favicon_id	favorites icon
moz_historyvisits	paces_id	moz_paces의 id
	visit_date	방문 시간

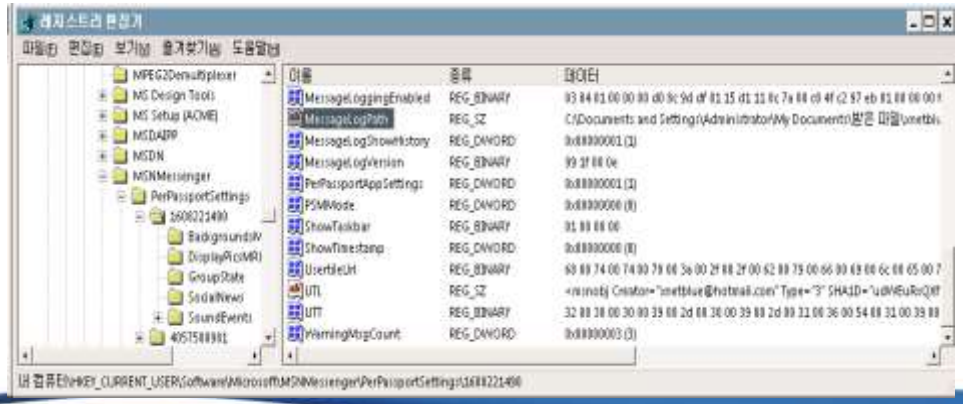
인터넷 메신저

- 대부분의 메신저는 설치 경로, 프로그램 버전 등의 정보를 레지스트리에 저장
- 설치 경로의 파악은 매우 중요
  - 일부 메신저는 대화내용을 메신저 설치 디렉토리 하위에 대화내용을 저장
  - 메신저 설정 파일 등의 핵심 파일이 프로그램이 설치된 경로에 존재



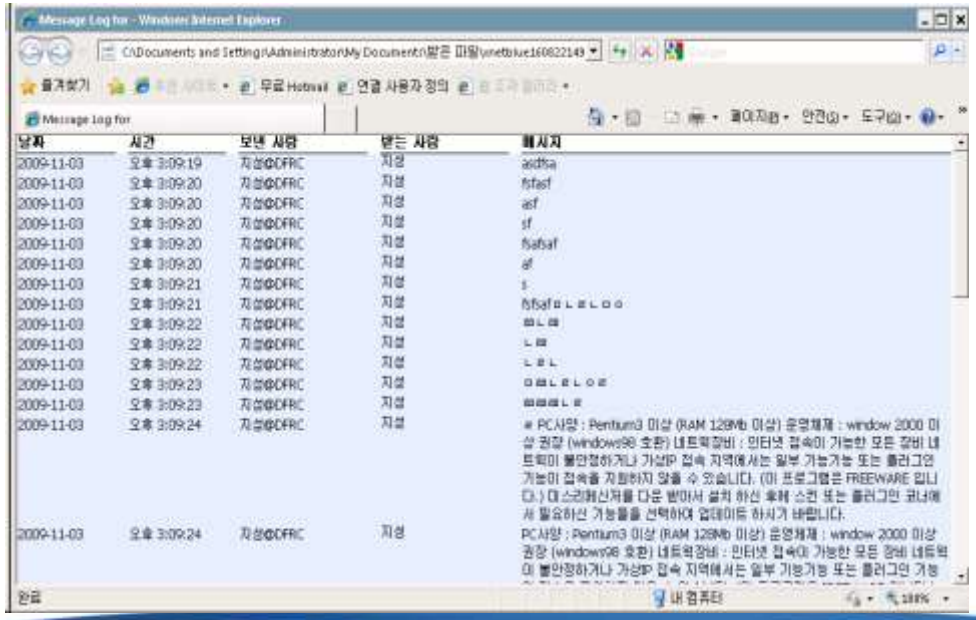
인터넷 메신저

- 설정 정보를 계정별로 레지스트리에 저장
  - 대화내역 저장 경로, 다운로드 파일 저장 경로, 자동 로그인 계정명 및 패스워드 등 저장
- 다운로드 파일 저장 경로를 통해 사용자가 다운로드 받은 파일을 확인 및 분석
- 자동 로그인 계정명을 통해 최종적으로 어떠한 계정을 사용하였는지 파악
- 특정 사용자를 가리기 위한 계정별 정보의 파악
  - 공용 PC의 경우에는 간혹 다수의 사용자가 짧은 시간 사용하는 경우



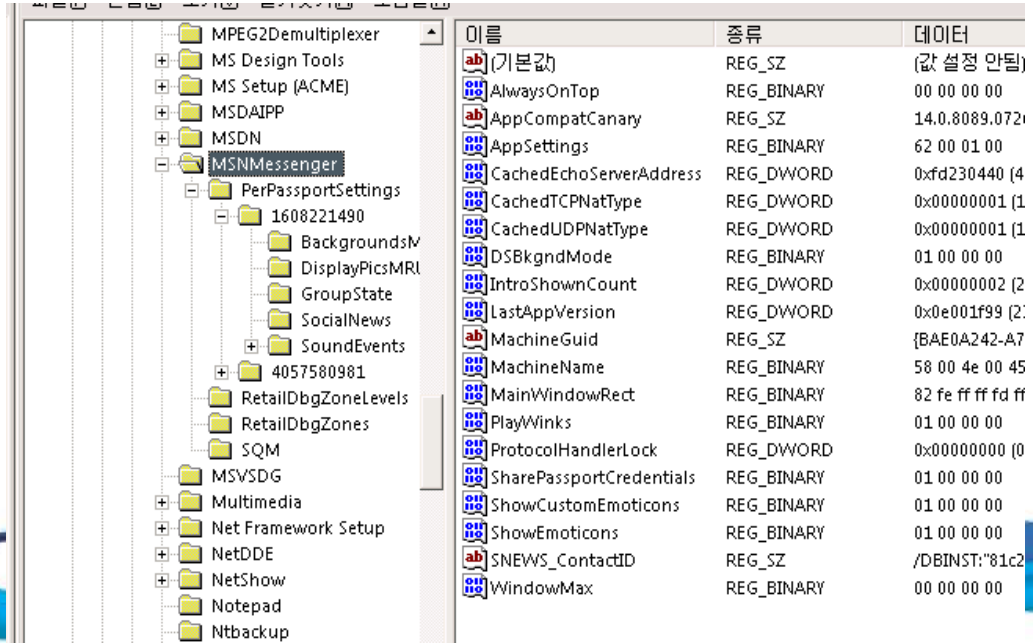
인터넷 메신저

- 대화를 저장하도록 설정하는 경우 대화내역이 PC에 저장
  - 일부 메신저는 대화 내역 암호화
  - Windows Live Messenger : 텍스트 형태 저장
- 실시간으로 대화 및 파일을 주고받을 수 있다는 장점
- 대화내역 및 파일 송수신 정보를 파악하는 일은 매우 중요
- 대화내역을 수집시 증거로써 쓰일 가능성이 매우 크다.



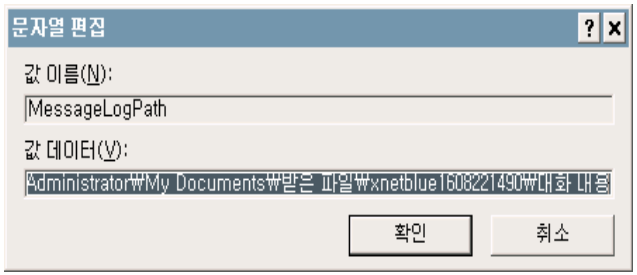
인터넷 메신저 – Windows Live Messenger

- Windows Live Messenger
  - HKCU₩Software₩Microsoft₩ MSNMessenger
  - 설치 경로, 프로그램 버전 및 기타 설정 정보들을 기록
  - “MachineGuid”값은 메신저가 설치된 PC의 GUID
  - "MachineName"은 PC의 이름
  - "PerPassportSettings“ :"DefaultMemberName"은 메신저 실행 후에 기본적으로 보이는 계정명
  - “SQM” : "TotalUpTime"은 로그인하여 사용한 총 시간(단위 : 초)



인터넷 메신저 – Windows Live Messenger

- "HKCU₩Software₩Microsoft ₩MSNMessenger₩PerPassportSettings"
  - 각 사용자를 구분하기 위한 Passport 번호로 하위키를 만들어 사용자별 계정정보를 기록
  - "MessageLogPath" 각 계정의 대화내역 정보가 저장되는 경로가 저장



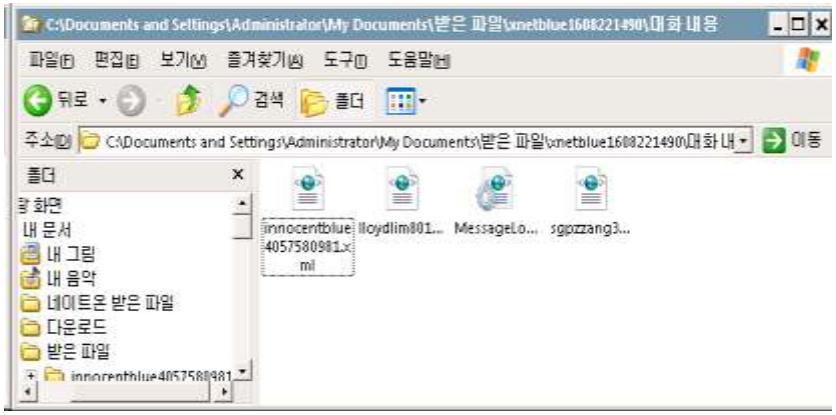
- 자동 로그인을 위한 계정 및 패스워드 정보
  - 윈도우 시스템의 Credential Management(자격 정보 관리)
    - advapi32.dll의 CredRead, CredEnumerate 함수 등을 통해 현재 활성화된 계정의 Credential 정보를 가져올 수 있다.

인터넷 메신저 – Windows Live Messenger

- CredRead, CredEnumerate 를 이용해 복구된 패스워드

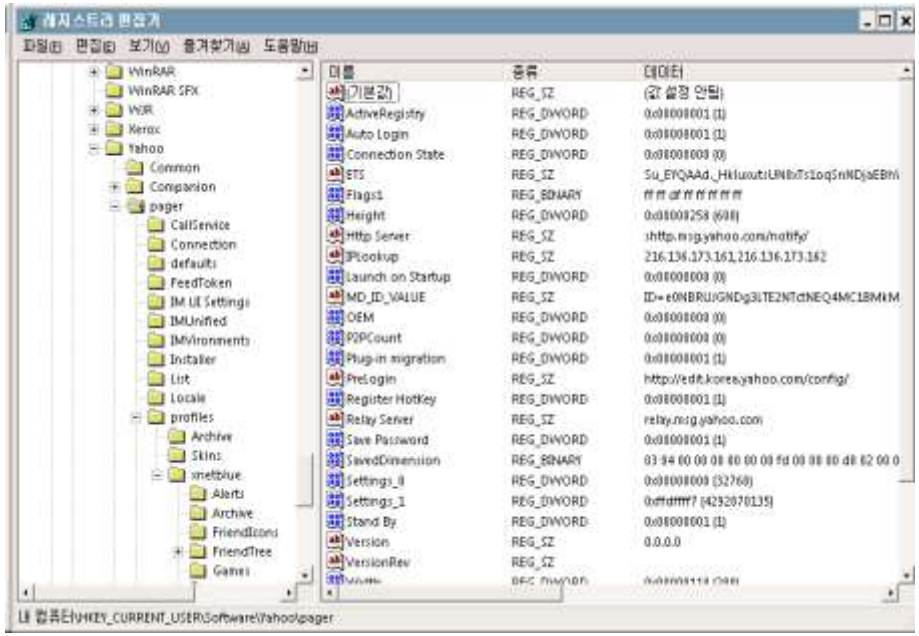
인터넷 메신저 – Windows Live Messenger

- Windows Live Messenger는 대화내역을 저장하는 경우, 앞서 설명한 계정별 정보 항목에서 확인 가능한 “MessageLogPath"에 저장되어 있는 경로에 XML 형식으로 저장하게 된다. 상대방 계정별로 ”계정명+Passport번호.xml"형식의 파일 이름을 갖게 되며, 해당 파일을 웹브라우저로 열어 쉽게 대화내역을 확인할 수 있다. 대화내역 파일에는 대화날짜, 시간, 보낸 사람, 받는 사람, 메시지 등의 항목이 저장된다.



인터넷 메신저 – Yahoo! Messenger

- Yahoo! Messenger는 윈도우 레지스트리의 “HKCU₩Software₩Yahoo₩pager" 키의 하위에 설치 경로, 프로그램 버전 및 기타 설정 정보들이 기록된다.

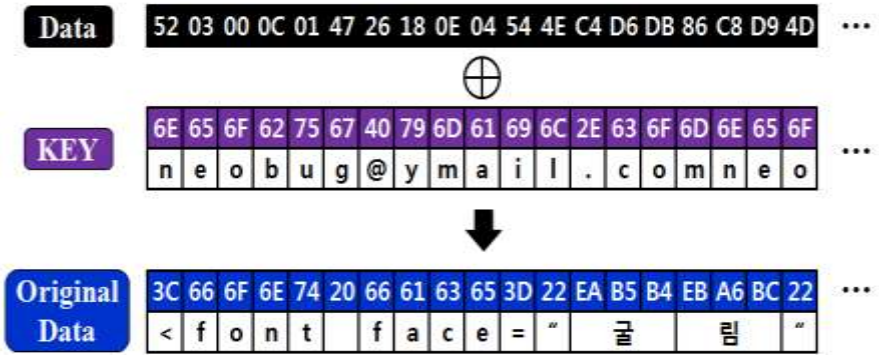


인터넷 메신저 – Yahoo! Messenger

- “Yahoo! User ID” : 가장 최근에 접속한 사용자의 계정명을 저장
- “HKCU₩Software₩Yahoo₩pager₩profiles”
  - 계정명과 같은 하위키가 생성, 한번이라도 접속을 시도했을 경우에 생성
  - 해당 계정 키 하위에 ”Alerts" 키의 "Total Login Tries" 값이 나타내는 데이터는 로그인이 실패했을 경우 총 몇 번의 로그인을 시도하였는지 나타낸다.

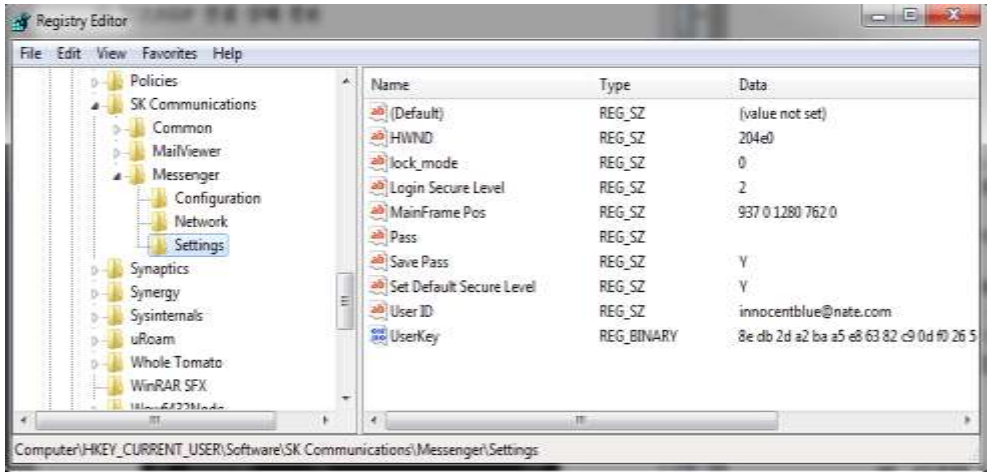
인터넷 메신저 – Yahoo! Messenger

- 대화내역 저장 옵션을 선택하는 경우에 한해 “<설치 경로>₩Profiles₩<사용자계정>₩Archive₩Messages₩<상대방계정>₩<년월일>-<사용자계정>.dat”의 경로에 대화내역 파일을 저장
- 대화내역 파일에서 추출한 대화 내용은 UTF-8로 인코딩
- 사용자 계정명과의 XOR(Exclusive OR)를 통해 저장



인터넷 메신저 – NateOn

- “HKCU₩Software₩SK Communications₩Messenger”
  - 설치 경로, 프로그램 버전 및 기타 설정 정보
- “Setting”
  - "UserID" 값에 최근에 접속한 계정을 저장
  - "UserKey” 항목으로 자동로그인을 위한 토큰을 저장
    - 사용자 PC의 MAC 주소 등의 고유한 정보를 통해 생성된다.



인터넷 메신저 – NateOn

- NateOn은 4.0으로 버전이 업그레이드 되면서, 기존에 파일로 저장되던 모든 대화 및 쪽지 내역이 외부 서버로 저장되도록 변경되어 해당 기록을 남기지 않는다. 따라서 로컬 시스템에서 획득할 수 있는 자료는 많지 않다.

Q & A