메신저 사용정보 분석을 통한 디지털 포렌식 기법 연구[1)]

*최준호 *권혁돈 *이상진 *임종인

고려대학교 정보경영공학전문대학원

*reaper91@cist.korea.ac.kr

Digital Forensic Technique Research through Messenger Analysis

*Choi, Joon-Ho *Kwon Hyuk-don *Lee Sang-jin *Lim Jong-in

Gruduate School of Information Management and Security, Korea University.

요약

메신저는 인터넷을 통해 실시간으로 대화를 주고받을 수 있는 소프트웨어로서 사용률이 점차 증가하고 있는 추세이다. 메신저의 사용률이 증가함에 따라 메신저를 사이버 범죄의 하나의 도구로써 이용하는 사례가 발생하고 있다. 메신저가 사이버 범죄에 악용되는 사례가 늘어나면서 전 세계적으로 MSN Messenger, AOL Instant Messenger, ICQ와 같은 외산 메신저 소프트웨어 대한 포렌식 연구가 활발히 진행 되고 있다. 본 논문에서는 현재 국내에서 사용되고 있는 메신저에 대한 포렌식 기법 연구를 통하여 범죄 발생 당시 용의자들의 정보를 획득하고 이를 컴퓨터 범죄 수사에 활용하는 방안을 제시한다

1. 서론

인터넷 사용자들에게 제공되고 있는 인터넷 메신저 프로그램은 종류가 다양하며, 각각의 메신저마다 각각 고유한 특성과 기능을 가지고 있어 메신저 분석에 어려움이 따른다. 따라서 여러 종류의 메신저들이 갖고 있는 공통적인 기능인 온라인으로 연결된 사용자간의 실시간 대화, 메신저를 통한 이메일 전송 등을 선정하여 우선적으로 분석한 후, 각각의 메신저에 특화된 분석 기법을 적용하여 분석을 수행해야 할 필요가 있다.

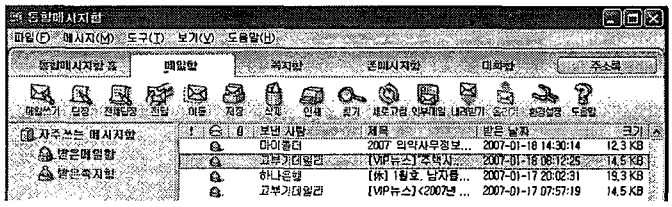
현재 인터넷 사용자들이 사용하는 메신저 프로그램 중 사용자들이 가장 많이 사용하고 있는 메신저는 Microsoft에서 개발한 MSN Messenger가 있으며 국내 사용자들이 가장 널리 많이 이용하는 메신저 프로그램에는 SK Communications에서 개발한 NateOn Messenger가 있다. 국내 사용자들은 국내 실정과 사용자 편의성 때문에 NateOn Messenger를 가장 많이 사용하고 있다.

본 논문에서는 국내에서 가장 많이 사용되고 있는 NateOn Messenger 소프트웨어에 대한 포렌식 기법 연구를 통하여, 사이버 범죄를 저지른 용의자가 메신저를 사용 했을 때 수사관이 얻을 수 있는 디지털 증거를 분석 하였다.

2. 네이트온 메신저 기본 구조

네이트온 메신저는 http://www.nate.com 사이트에서 사용자의 개인정보를 입력한 뒤 가입하면 무료로 이용할 수 있으며, 2007년 2월 SK Communications의해 버전 v3.5.16.2 (616)가 사용자들에게 정식 배포되고 있다. v3.5.16.2 (616)버전의 네이트온 메신저를 기본설정으로 메신저를 설치했을 경우 네이트온 메신저와 관련된 파일이 설치되는 디렉터리, 네이트 온 메신저가 사용하는 레지스트리 키와 키 값은 다음과 같다.

가. 네이트 온 관련 파일, 디렉터리



[그림 1] 네이트 온 통합 메시지 함

1. 설치 디렉터리 : 네이트온 메신저는 기본으로 \Program Files\NATEON 디렉터리에 설치된다.

2. 사용자 계정 디렉터리 : 네이트온 메신저는 자체적으로 사용하는 랜덤 데이터 생성 알고리즘을 사용하여 네이트온을 이용하는 사용자의 ID를 랜덤 데이터로 가공하여 사용자 계정정보와 관련된 디렉터리명과 레지스트리 키 값으로 이용하고 있다. 따라서 사용자 계정관련 파일은 다음과 같이 랜덤 데이터로 생성된 디렉터리 명을 가진 디렉터리의 하위 디렉터리에 위치한다.
ProgramFiles\NATEON20\BIN\3F54B6EC3FAE31061F5E79A72A9B649A\[ID]

3. 사용자 설정 파일 : 네이트온 메신저를 이용하는 각각의 사용자가 설정한 메신저의 설정사항을 저장한 파일(nateon_pref_u.ini)은 사용자 계정 디렉터리에 위치한다.

4. 메일 보관함 디렉터리 : 네이트온을 통해 주고받은 메일을 사용

1) 본 연구는 과학재단 디지털 정보 획득 기반기술 연구(M10640010005-06N4001-00500)의 지원으로 수행되었습니다.

계정 디렉터리의 하위 폴더인 maildata에 위치한다.

5. 쪽지 보관함 디렉터리 : 네이트온을 통해 주고받은 쪽지는 사용자 계정 디렉터리의 하위 폴더인 memodata에 위치한다.

6. 대화 보관함 디렉터리 : 네이트온을 통해 주고받은 대화는 사용자 계정 디렉터리의 하위 폴더인 chatdata에 위치한다.

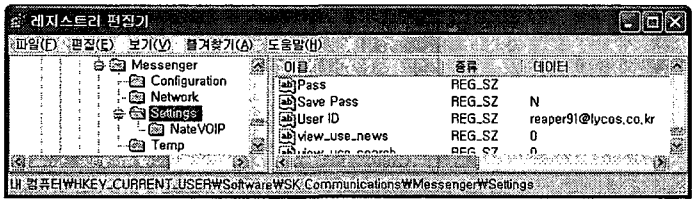
7. 쿠키 파일 : 네이트온을 사용한 사용 내역을 기록한 쿠키 데이터는 Documents and Settings\[시스템 로그인 계정]\Cookies\[ID].txt로 저장된다.

8. 받은 파일 디렉터리 : 네이트온을 통해 주고받은 파일은 기본 설정시 Documents and Settings\[시스템 로그인 계정]\My Documents\[네이트온 받은 파일] 디렉터리에 저장된다.

나. 네이트 온 관련 레지스트리 값

사용자 계정 레지스트리 값 :

네이트 온의 사용자 계정과 관련된 레지스트리 값은 HKCU\Software\SK Communications\Messenger\Settings 에 저장된다.



[그림 2] 네이트 온의 사용자 계정 레지스트리 값

그림2의 네이트 온의 사용자 계정 레지스트리의 키에는 각각 마지막으로 네이트온 메신저에 로그인 한 사용자 ID(User ID), 자동 로그인 여부(Save Pass), 자동 로그인 설정을 하였을 경우 사용자의 비밀번호가 암호화된 문자열(Pass)의 키 값이 저장된다.

3. 네이트 온 프로세스 메모리 분석

네이트온 메신저 프로그램이 실행되고 있는 도중 생성되는 프로세스의 메모리 분석을 통하여 사용자의 인터넷 사용자 내역, 사용자가 접근한 파일, 사용자의 쿠키 데이터, 사용자가 주고받은 메시지 등을 알아 낼 수 있다.

가. 사용자의 인터넷 사용 내역

네이트온 프로세스 메모리에서 용의자가 사건 발생 당시 방문한 인터넷 사이트를 추출하여 용의자의 인터넷 사용내역을 알아 낼 수 있다. 용의자자 방문한 인터넷 사이트 정보는 임의의 프로세스 메모리 영역에서 다음과 같은 포맷을 가지고 있다.

Visited : [사용자 ID]@http://www.target.com

```
0000 0000 0000 0000 0000 000D F0AD 0B56|..............V
6973 6974 6564 3A20 7265 6170 6572 3931|isited: reaper91
4068 7474 703A 2F2F 7777 772E 6576 6964|@http://www.evid
656E 6365 2D65 6C69 6D69 6E61 746F 722E|ence-eliminator.
636F 6D2F 7072 6F64 7563 742E 7368 746D|com/product.shtm
6C00 0B10 0002 0000 0000 0000 0000 0000|l...............
```

[그림 3] 용의자가 방문한 사이트 1

```
0000 0000 0000 0000 0000 000D F0AD 0B56|..............V
6973 6974 6564 3A20 7265 6170 6572 3931|isited: reaper91
4068 7474 703A 2F2F 7777 772E 6372 6163|@http://www.crac
6B73 6461 7461 2E63 6F6D 2F67 6574 2E70|ksdata.com/get.p
6870 3F69 643D 3831 3537 3300 F0AD 0B10|hp?id=81573.....
0002 0000 0000 1000 0000 0000 0000 0088|................
```

[그림 4] 용의자가 방문한 사이트 2

네이트온 프로세스에서 추출한 데이터[그림 3, 그림 4]를 통하여 용의자가 방문한 사이트가 다음과 같음을 알 수 있다.

http://www.cracksdata.com/get.php?id=81573

http://www.evidence-eliminator.com/product.shtml

나. 사용자가 접근한 파일

네이트온 프로세스 메모리에서 용의자가 사건 발생 당시 접근한 파일 목록을 추출하여 용의자가 범죄에 이용한 파일들을 알아 낼 수 있다. 용의자가 접근한 파일 목록 정보는 임의의 프로세스 메모리 메모리 영역에서 다음과 같은 포맷을 가지고 있다.

Visited : [사용자 ID]@file:파일명

```
0000 0000 0000 0000 0000 000D F0AD 0B56|..............V
6973 6974 6564 3A20 7265 6170 6572 3931|isited: reaper91
4066 696C 653A 2F2F 2F43 3A2F 4465 6375|@file:///C:/Docu
6D65 6E74 7325 3230 616E 6425 3230 5365|ments%20and%20Se
7474 696E 6773 2F72 6561 7065 7239 312F|ttings/reaper91/
B9D9 C5C1 2532 3043 ADB8 E92F 4576 6964|....%20..../Evid
656E 6365 5F45 6C69 6D69 6E61 746F 725F|ence_Eliminator_
7635 2E30 2E35 335F 6279 5F54 4D47 2E7A|v5.0.53_by_TMG.z
6970 0010 0002 0000 0000 1000 0000 0000|ip..............
```

[그림 5] 용의자가 접근한 파일 1

```
0000 0000 0000 0000 0000 000D F0AD 0B56|..............V
6973 6974 6564 3A20 7265 6170 6572 3931|isited: reaper91
4066 696C 653A 2F2F 2F43 3A2F 5072 6F67|@file:///C:/Prog
7261 6D25 3230 4669 6C65 732F 4576 6964|ram%20Files/Evid
656E 6365 2532 3045 6C69 6D69 6E61 746F|ence%20Eliminato
722F 4865 6C70 2F65 652E 6368 6D00 0B10|r/Help/ee.chm...
0002 0000 0000 1000 0000 0000 0000 0000|................
```

[그림 6] 용의자가 접근한 파일 2

네이트온 프로세스에서 추출한 데이터[그림 5, 그림 6]을 통하여 용의자가 접근한 파일이 Evidence_Eliminator_v5.0.53_by_TMG.zip, ee.chm 임을 알 수 있다,.

다. 사용자의 쿠키 데이터

네이트온 프로세스 메모리에서 용의자의 쿠키 데이터를 추출하여 용의자가 방문한 인터넷 사이트와 계정정보를 알아 낼 수 있다. 용의자의 쿠키 데이터 정보는 임의의 프로세스 메모리 영역에서 다음과 같은 포맷을 가지고 있다.

Cookie : [사용자 ID]@쿠키 파일 이름

```
ADOB 436F 6F6B 6965 3A72 6561 7065 7239|..Cookie:reaper9
3140 3231 302E 3232 302E 3136 312E 3730|1@210.220.161.70
2F00 7265 6170 6572 3931 4032 3130 2E32|/.reaper91@210.2
3230 2E31 3631 5B32 5D2E 7478 7400 0DF0|20.161[2].txt...
ADOB 0DF0 ADOB 0DF0 ADOB 0DF0 ADOB 0DF0|................
```

[그림 7] 용의자의 쿠키 정보 1

```
ADOB 436F 6F6B 6965 3A72 6561 7065 7239|..Cookie:reaper9
3140 7777 772E 7375 7065 7275 7365 722E|1@www.superuser.
636F 2E6B 722F 00F0 ADOB 7265 6170 6572|co.kr/....reaper
3931 4077 7777 2E73 7570 6572 7573 6572|91@www.superuser
2E63 6F5B 325D 2E74 7874 00F0 ADOB 0DF0|.co[2].txt......
```

[그림 8] 용의자의 쿠키 정보 2

네이트온 프로세스에서 추출한 데이터[그림 7, 그림 8]을 통하여 용의자가 방문한 사이트와 계정정보가

210.220.161.70, reaper91

http://www.superuser.com, reaper91

임을 알 수 있다.

다. 사용자가 주고받은 메시지 데이터

네이트온 프로세스 메모리에서 용의자가 주고받은 메시지를 추출하여 용의자가 다른 사람과 나눈 메시지를 알아낼 수 있다.

1. 용의자가 오프라인의 네이트온 메신저 사용자에게 메시지를 전송 하였을 경우 프로세스 메모리에서 용의자가 전송한 메시지 정보를 가진 부분은 다음과 같은 포맷을 가지고 있다.

w.send&cmn=904348191&

id=[메시지를 송신하는 사용자 ID]&

uuid=73981c15-4878-4af2-a79f-675509dfc76a&

to_ids=[메시지를 수신하는 사용자 그룹]&

ticket=[예약된 메시지의 순번]&

subject=[메시지 명]&

to_id=[메시지를 수신하는 사용자의 ID]&

content_type=text&

content=[메시지 데이터]&

confirm=[메시지 확인 여부]

```
16878128|0802 A002 7709 7365 6E64 2663 6D6E 3D39|....w.send&cmn=9
16878144|3034 3334 3831 3931 2669 643D 7265 6170|04348191&id=reap
16878160|6572 3931 406C 7963 6F73 2E63 6F2E 6B72|er91@lycos.co.kr
16878176|2675 7569 643D 3733 3938 3163 3135 2D34|&uuid=73981c15-4
16878192|3837 382D 3461 6632 2D61 3739 662D 3637|878-4af2-a79f-67
16878208|3535 3039 6466 6337 3661 2674 6F5F 6964|5509dfc76a&to_id
16878224|733D 6D69 7269 2D68 6170 7079 406F 7267|s=miri-happy@org
16878240|696F 2E6E 6574 2674 6963 6B65 743D 4438|io.net&ticket=D8
16878256|3430 4646 4234 3632 3638 3541 3431 3344|40FFB462685A413D
16878272|3241 3939 4946 3831 3442 4642 4338 3842|2A99CF814BFBC88B
```

〔그림 9〕 용의자가 송신한 메시지 1

```
16878592|3437 3335 4331 3643 4146 3042 4645 3039|4735C16CAF0BFE09
16878608|3734 3938 4239 3138 3230 3430 4338 2673|7498B9182040C8&s
16878624|7562 6A65 6374 3D52 4541 5045 5239 3153|ubject=REAPER91S
16878640|454E 444D 5347 2674 6F5F 6964 3D6D 6972|ENDMSG&to_id=mir
16878656|692D 6861 7070 7940 6F72 6769 6F2E 6E65|i-happy@orgio.ne
16878672|7426 636F 6E74 656E 745F 7479 7065 3D74|t&content_type=t
16878688|6578 7426 636F 6E74 656E 743D 5245 4150|ext&content=REAP
16878704|4552 3931 5345 4E44 4D53 4726 636F 6E66|ER91SENDMSG&conf
16878720|6972 6D3D 4E02 FFFF FFFF 0000 0000 0000|irm=N.........
```

〔그림 10〕 용의자가 송신한 메시지 2

네이트온 프로세스에서 추출한 데이터[그림 9, 그림 10]를 통하여 용의자가 오프라인 사용자에게 송신한 메시지가 'REAPER91SENDMSG' 임을 알 수 있다.

2. 용의자가 온라인 네이트온 메신저 사용자와 실시간 메시지를 주고은 경우 프로세스 메모리에서 용의자가 실시간 메시지를 주고받은 정보는 임의의 프로세스 메모리 영역에서 다음과 같은 포맷을 가지고 있다.

title:[메시지 명]

from:[메시지를 송신하는 사용자 ID]

ref:[메시지를 수신하는 사용자 ID]

date:[메시지를 주고받은 시간]

session_id:2752878

uuid:63bd405f-5af0-4ad5-aba5-ccd2fa64d00e

contenttype: [메시지 타입]

length: [메시지 길이]

font-name: [폰트 이름]

font-style: [폰트 형태]

font-size: [폰트 크기]

font-color: [폰트 색]

[메시지 데이터]

```
2500 9400 2501 0802 90DC 1101 0D0A 7469|%...%.........ti
746C 653A 5245 4150 4552 3931 5345 4E44|tle:REAPER91SEND
4D53 470D 0A66 726F 6D3A 7265 6170 6572|MSG..from:reaper
3931 406C 7963 6F73 2E63 6F2E 6B72 0D0A|91@lycos.co.kr..
7265 663A 7769 7365 6D61 6E39 3140 6E61|ref:wiseman91@na
7465 2E63 6F6D 0D0A 6461 7465 3A32 3030|te.com..date:200
3730 3231 3430 3734 3831 350D 0A73 6573|70214074815..ses
7369 6F6E 5F69 643A 3237 3532 3837 380D|sion_id:2752878.
0A75 7569 643A 3633 6264 3430 3566 2D35|.uuid:63bd405f-5
6166 302D 3461 6435 2D61 6261 352D 6363|af0-4ad5-aba5-cc
6432 6661 3634 6430 3065 0D0A 636F 6E74|d2fa64d00e..cont
656E 7474 7970 653A 7465 7874 0D0A 6C65|enttype:text..le
6E67 7468 3A33 300D 0A66 6F6E 742D 6E61|ngth:30..font-na
6D65 3AEA B5B4 EBA6 BC0D 0A66 6F6E 742D|me:.....font-
7374 796C 653A 2530 300D 0A66 6F6E 742D|style:%00..font-
7369 7A65 3A31 300D 0A66 6F6E 742D 636F|size:10..font-co
6C6F 723A 2330 3530 3530 350D 0A0D 0A52|lor:#050505....R
4541 5045 5239 3153 454E 444D 5347 2000|EAPER91SENDMSG .
```

〔그림 11〕 용의자가 주고받은 메시지 1

```
300D 0A49 4D53 470D 0A74 6974 6C65 3A57|0..IMSG..title:W
4953 454D 414E 3931 5345 4E44 4D53 470D|ISEMAN91SENDMSG.
0A66 726F 6D3A 7769 7365 6D61 6E39 3140|.from:wiseman91@
6E61 7465 2E63 6F6D 0D0A 7265 663A 7265|nate.com..ref:re
6170 6572 3931 406C 7963 6F73 2E63 6F2E|aper91@lycos.co.
6B72 0D0A 6461 7465 3A32 3030 3730 3231|kr..date:2007021
3430 3734 3833 390D 0A73 6573 7369 6F6E|4074839..session
5F69 643A 3332 3832 3630 0D0A 7575 6964|_id:328260..uuid
3A35 3239 3766 3533 392D 6161 6437 2D34|:5297f539-aad7-4
3338 622D 6231 6662 2D36 3034 3964 3535|38b-b1fb-6049d55
6638 6538 310D 0A63 6F6E 7465 6E74 7479|f8e81..contentty
7065 3A74 6578 740D 0A6C 656E 6774 683A|pe:text..length:
3332 0D0A 666F 6E74 2D6E 616D 653A EAB5|32..font-name:..
B4EB A6BC 0D0A 666F 6E74 2D73 7479 6C65|......font-style
3A25 3030 0D0A 666F 6E74 2D73 697A 653A|:%00..font-size:
3130 0D0A 666F 6E74 2D63 6F6C 6F72 3A23|10..font-color:#
3035 3035 3035 0D0A 0D0A 5749 5345 4D41|050505....WISEMA
4E39 3153 454E 444D 5347 2000 9E98 EB90|N91SENDMSG .....
```

〔그림 12〕 용의자가 주고받은 메시지 2

네이트온 프로세스에서 추출한 데이터[그림 11, 그림 12]를 통하여 용의자가 다른 네이트온 메신저 사용자와 주고받은 메시지가 다음과 같음을 알 수 있다.

[그림 11]의 송신자, 수신자, 메시지

송신자 : reaper91 수신자 : wiseman91

메시지 : REAPER91SENDMSG

[그림 12]의 송신자 수신자 메시지

송신자 : reaper91 수신자 : wiseman91

메시지 : WISEMAN91SENDMSG

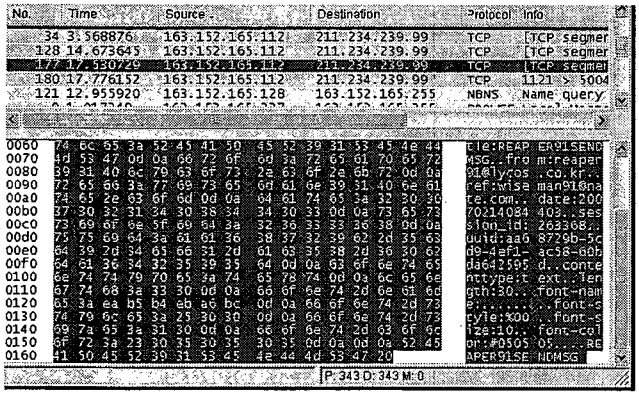
4. 네이트 온 인터넷 통신 분석

네이트온 메신저 프로그램 간의 통신 패킷을 모니터링, 분석하여 용의자와 다른 네이트온 메신저 사용자의 메시지 송수신을 실시간으로 확인 할 수 있다.

네이트온 메신저 프로그램의 메시지 송수신은 HTTP, TCP 프로토콜을 사용하며, 통신에서 주고받는 메시지의 포맷은 프로세스 메모리 영역에서 사용하는 포맷을 그대로 사용한다. 그리고 포맷을 하나의 데이터로 취급하여 HTTP, TCP 프로토콜을 통해 전송한다.

네이트온 인터넷 통신에서도 역시 용의자가 오프라인 사용자에게 메시지를 전송하였을 경우와, 온라인 사용자에게 메시지를 전송하였을

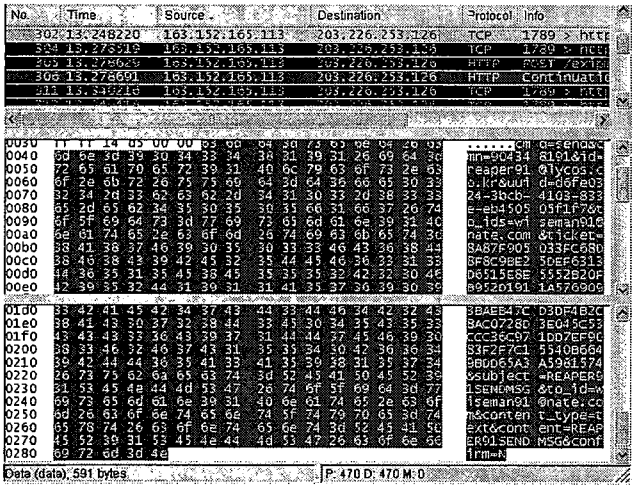
경우가 있다. 온라인 사용자에게 메시지를 전송하는 경우 TCP 프로토콜을 이용하여 실시간 전송을 하고, 오프라인 사용자에게 메시지를 전송하는 경우에는 HTTP 프로토콜을 통해 메시지를 네이트온 사이트에서 수신자가 네이트온에 로그인시 메시지를 확인 시켜준다.



〔그림 13 온라인 사용자에게 메시지 전송〕

[그림 13]을 통해 163.152.165.112 컴퓨터에서 네이트온 메신저를 사용하고 있는 용의자가 온라인 네이트온 사용자 wisemans91에게 다음과 같은 메시지를 송신한 것을 알 수 있다.

REAPER91SENDMSG



〔그림 14 오프라인 사용자에게 메시지 전송〕

[그림 13]을 통해 163.152.165.113 컴퓨터에서 네이트온 메신저를 사용하고 있는 용의자가 다른 오프라인 네이트온 사용자 wiseman91에게 다음과 같은 메시지를 송신한 것을 알 수 있다.

REAPER91SENDMSG

5. 결론

메신저 사용정보 분석을 통한 디지털 포렌식 기법 연구를 기반으로 한 메신저 프로그램의 프로세스 메모리 영역분석과 통신 패킷분석을 이용한 포렌식 정보 수집은 포렌식 수사에 있어서 다음과 같이 활용될 수 있다.

용의자가 방문한 사이트를 목록화하여 용의자의 인터넷 사용내역을 확인할 수 있다. 용의자가 접근한 파일목록을 점검하여 용의자가 범죄에 이용에 사용했던 프로그램 파일을 발견할 수 있다. 용의자의 쿠키 정보를 통해 용의자가 방문한 사이트와 그에 대한 계정을 확인할 수 있다. 용의자가 다른 사용자와 주고받은 메시지를 분석하여 범행 동기, 범행 시기, 범행 대상, 범행 방법을 유추 할 수 있다.

메신저 프로그램 통신 네트워크 실시간 모니터링이 가능한 환경에을 바탕으로 하여 용의자의 범죄 행위를 포렌식 수사관이 예방, 방지할 수 있다.

향후 계획으로는 네이트온 메신저 프로그램의 심도있는 분석과, 다양한 메신저 프로그램의 기능과 특성을 파악하여 각각 포렌식 수사에 활용할 수 있는 정보 추출 기법을 연구하는 것이다.

[참고문헌]

〔1〕 NateOn Messenger

http://www.nate.com/

〔2〕 Window User Mode Process Dumper

http://www.microsoft.com/

〔3〕 Ethereal : A Network Protocol Analyzer

http://www.ethereal.com/

〔4〕 The Hex Workshop Hex Editor

http://www.hexworkshop.com/

〔5〕 Mike Dickson "An examination into MSN Messenger 7.5 contact identification" Digital Investigation, 2006.