

# BOB 챌린지: 디지털 포렌직 챌린지

A faint world map is centered in the background, showing the continents of North America, South America, Europe, and Africa. The map is rendered in a light gray color against a slightly darker gray background. At the bottom of the image, there is a grid pattern of thin white lines, suggesting a floor or a digital interface. The overall aesthetic is clean and modern.

포렌식이란?

# 포렌식이란?

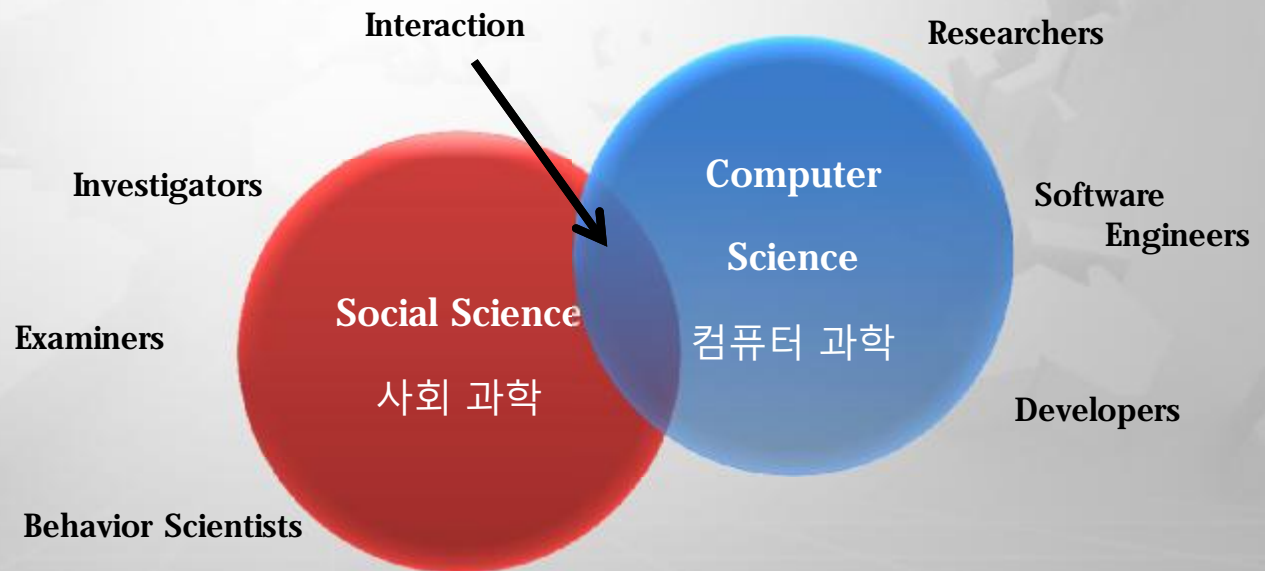
## 포렌식(Forensics)

범죄 사실을 규명하기 위해 각종 증거를 과학적으로 분석하는 분야

법의학 또는 법과학(Forensic Science)

## 디지털 포렌식(Digital Forensics)

디지털 분야에서 디지털 기기에 남아있는 각종 데이터를 조사하여 사건을 규명하는 분야



## 전문가간의 대립: 주어진 증거물에 대한 사실 발견/해석

### 의사 부인 박씨의 사망당시 욕실 상황

귀 뒤쪽에서 턱쪽이 아니라 뒤통수쪽으로 흐른 핏자국

뒤통수 1.5cm 찢어진 상처. 사인은 아닌 것으로 판명

심장·간 등 주요 장기에 질병 흔적 없음

### 결국 국과수가 캐나다 법의학 전문가 이겼다

### 재판 과정의 주요 쟁점에 대한 법원 판단

피고인 백씨 측 주장	쟁점	검찰 수사와 1심 판결
이상 자세로 질식사	사망원인	목이 졸려 질식사
오랜 시간 목이 눌린 자세에서 피가 통하지 않아 생긴 흔적	시신 목 부위 피부 까짐과 내부 출혈	목을 졸려 살해당한 전형적인 흔적
욕조에 넘어진 뒤 고개가 흔들리면서 피가 흐르는 방향이 바뀐 것	얼굴의 핏자국 중 귀 뒤쪽에서 뒤통수 쪽으로 흐른 자국	침대에 누운 상태에서 목이 졸린 증거
사후에 생긴 시반(屍斑·피가 쏠려 생기는 반점)	시신의 상처와 멍	목이 졸리며 반향한 흔적
DNA는 평소 생활 과정에서 묻은 것	침대에서 발견된 소변 흔적과 DNA	침대에서 살해됐다는 증거

숨진 박씨의 목 부위에 졸린 흔적이 있고, 시신 여러 부위에 상처와 멍이 나 있었기에 **국립과학수사연구원에 부검을 의뢰**하는 등 추가 수사에 나섰다. 경찰은 평소 백씨가 게임 중독 증세를 보여 아내와 자주 다툼을 벌였고, 사건 전날에도 전문의 시험을 친 뒤 새벽까지 게임을 한 점 등으로 미뤄 백씨가 사건 당일 새벽 아내와 다투다가 우발적으로 살해한 것으로 보고 백씨를 구속했다.

재판 과정에서 남편 백씨와 변호인은 박씨의 사인을 '이상(異常) 자세에 의한 질식사'라고 주장했다. 시신의 목이 졸린 흔적은 오랜 시간 욕실 안에 목이 눌린 자세로 있어 피가 통하지 않아 생긴 흔적이라는 논리를 폈다.

변호인 측은 지난 7월 **캐나다 토론토대 법의학센터장인 마이클 스벤 폴라넨(Pollanen·43) 박사**를 증인으로 내세워 국과수의 부검 결과에 집중적으로 의문을 제기했다. 폴라넨 박사는 법정에서 "잘 훈련된 법의학관이라도 최종 단계에서 이상 자세에 의한 질식에 따른 울혈(鬱血·피가 몰림)을 목 졸림에 의한 것이라고 잘못 판단할 수가 있다"고 주장했다.

재판부는 그러나 폴라넨 박사의 주장에 대해 "판단 증거로 제시한 논문에 인용된 사례는 **만성질환으로 사망한 82세 노인**으로 시신 자세도 이번 사건과 다르다. 또 검찰 증거로 제출된 부검 사진을 본 뒤 '(변호인 측에서) 받은 사진은 상태가 안 좋아서 잘못 판단한 것 같다'고 말하는 등 (폴라넨 박사의) 주장에 타당성이 부족하다"고 밝혔다.

## 로카르의 법칙(Locard's Principle)

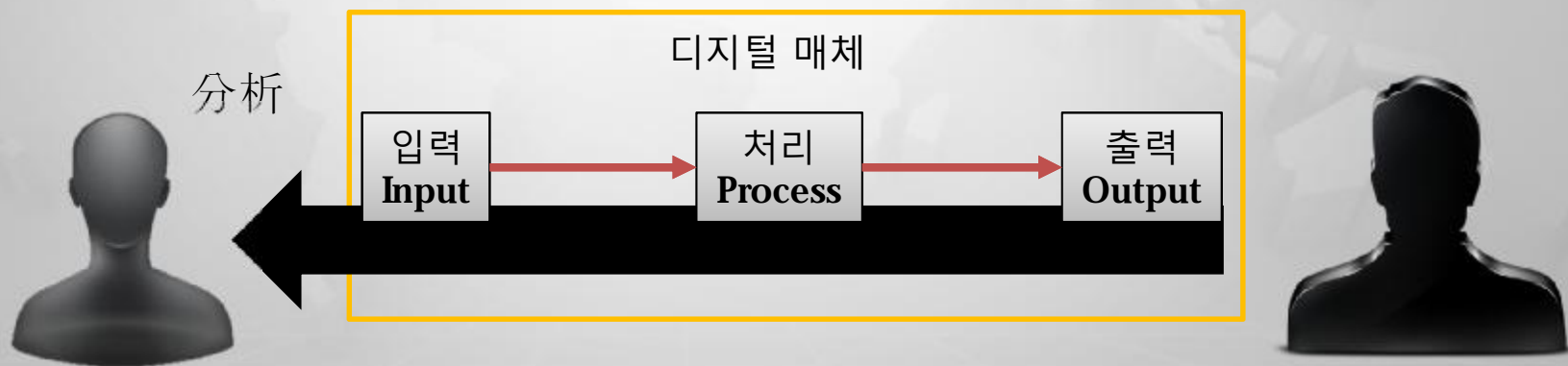
“접촉하는 두 개체는 서로 흔적을 주고받는다.”

에드몽 로카르

- 리옹대학에서 의학과 법학 공부, 어린 시절부터 코난 도일의 셜록 홈즈를 매우 좋아함.
- **1910**년 에는 독자적인 범죄학 연구소 열어 많은 사건 해결
- 지문 속의 지문 : 사람의 지문을 따라 난 땀구멍의 수가 지문만큼이나 사람에 따라 다르다.

범죄를 저지른 사람은 자신도 모르게 범죄 현장에 단서를 남기고 현장에 있던 어떤 것을 가지고 있다고 본 것이다. 전세계 과학수사요원들이 원칙으로 삼는 법칙이다. 그는 현대 과학수사에 큰 영향을 끼쳤다.

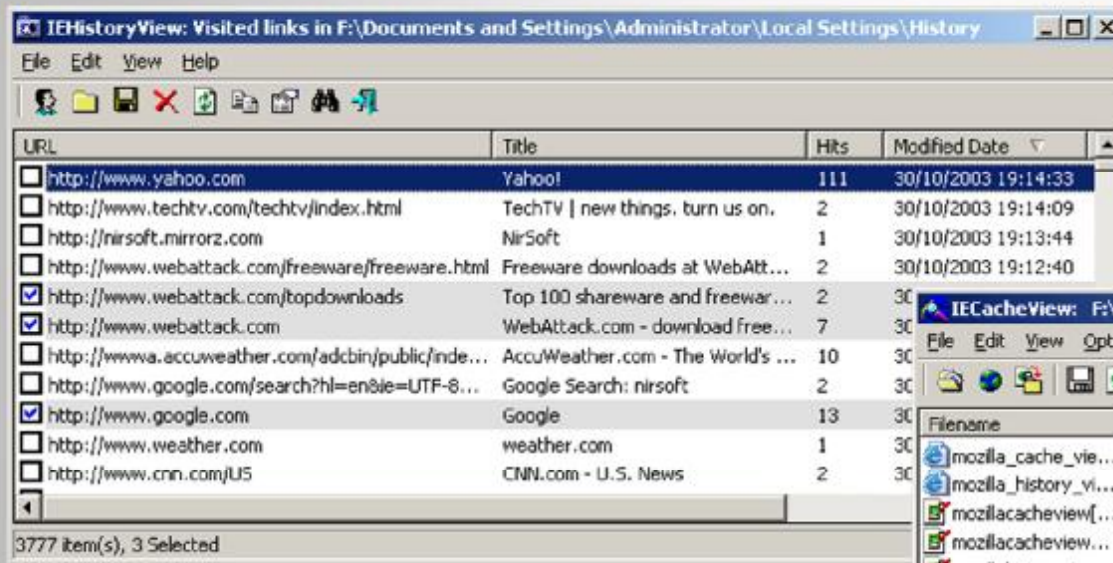
## 로카르의 법칙 in 디지털 포렌식



분석: 얽혀 있거나 복잡한 것을 풀어서 개별적인 요소나 성질로 나눔.

## 윈도우 분석 예제: 인터넷 히스토리

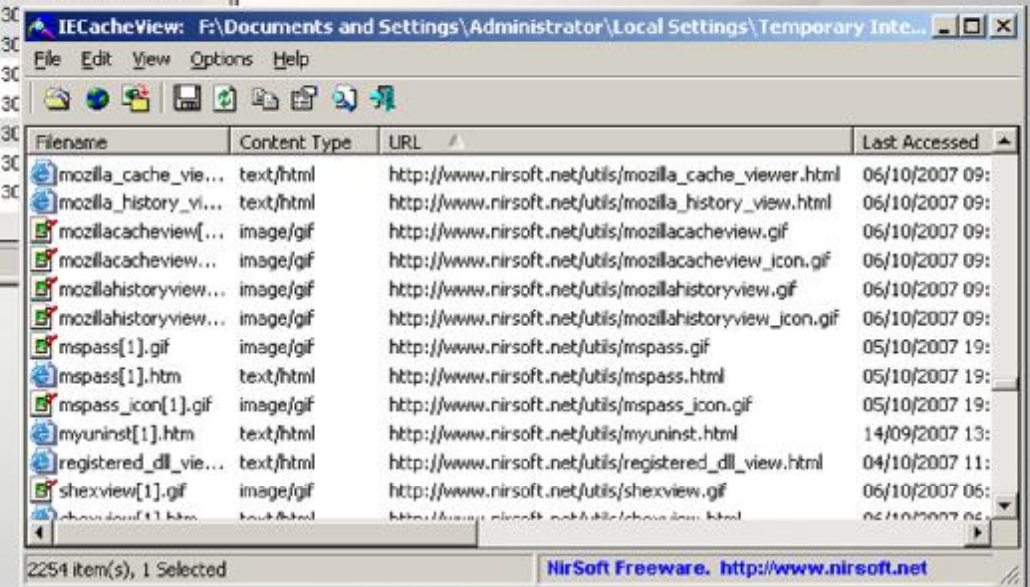
인터넷 히스토리 목적은 한번 방문한 페이지를 재 방문할 경우 **Internet Explorer** 상에서 로딩 속도를 빠르게 하기 위한 캐시 역할을 한다. **index.dat** 파일은 쿠키, 히스토리, 인터넷임시파일 폴더의 정보가 기록되어 있기 때문에 사용자의 인터넷 사용 패턴이나 접속 기록 등을 확인할 수 있다.



URL	Title	Hits	Modified Date
<input type="checkbox"/> http://www.yahoo.com	Yahoo!	111	30/10/2003 19:14:33
<input type="checkbox"/> http://www.techtv.com/techtv/index.html	TechTV   new things. turn us on.	2	30/10/2003 19:14:09
<input type="checkbox"/> http://nirsoft.mirrorz.com	NirSoft	1	30/10/2003 19:13:44
<input type="checkbox"/> http://www.webattack.com/freeware/freeware.html	Freeware downloads at WebAtt...	2	30/10/2003 19:12:40
<input checked="" type="checkbox"/> http://www.webattack.com/topdownloads	Top 100 shareware and freewar ...	2	30/10/2003 19:12:40
<input checked="" type="checkbox"/> http://www.webattack.com	WebAttack.com - download free ...	7	30/10/2003 19:12:40
<input type="checkbox"/> http://www.accuweather.com/adcbn/public/inde...	AccuWeather.com - The World's ...	10	30/10/2003 19:12:40
<input type="checkbox"/> http://www.google.com/search?hl=en&ie=UTF-8...	Google Search: nirsoft	2	30/10/2003 19:12:40
<input checked="" type="checkbox"/> http://www.google.com	Google	13	30/10/2003 19:12:40
<input type="checkbox"/> http://www.weather.com	weather.com	1	30/10/2003 19:12:40
<input type="checkbox"/> http://www.cnn.com/US	CNN.com - U.S. News	2	30/10/2003 19:12:40

3777 item(s), 3 Selected

[www.nirsoft.net](http://www.nirsoft.net)



Filename	Content Type	URL	Last Accessed
mozilla_cache_vie...	text/html	http://www.nirsoft.net/utis/mozilla_cache_viewer.html	06/10/2007 09:
mozilla_history_vi...	text/html	http://www.nirsoft.net/utis/mozilla_history_view.html	06/10/2007 09:
mozillacacheview(...)	image/gif	http://www.nirsoft.net/utis/mozillacacheview.gif	06/10/2007 09:
mozillacacheview(...)	image/gif	http://www.nirsoft.net/utis/mozillacacheview_icon.gif	06/10/2007 09:
mozillahistoryview...	image/gif	http://www.nirsoft.net/utis/mozillahistoryview.gif	06/10/2007 09:
mozillahistoryview...	image/gif	http://www.nirsoft.net/utis/mozillahistoryview_icon.gif	06/10/2007 09:
mypass[1].gif	image/gif	http://www.nirsoft.net/utis/mypass.gif	05/10/2007 19:
mypass[1].htm	text/html	http://www.nirsoft.net/utis/mypass.html	05/10/2007 19:
mypass_icon[1].gif	image/gif	http://www.nirsoft.net/utis/mypass_icon.gif	05/10/2007 19:
myuninst[1].htm	text/html	http://www.nirsoft.net/utis/myuninst.html	14/09/2007 13:
registered_dll_vie...	text/html	http://www.nirsoft.net/utis/registered_dll_view.html	04/10/2007 11:
shexview[1].gif	image/gif	http://www.nirsoft.net/utis/shexview.gif	06/10/2007 06:
shexview[1].htm	text/html	http://www.nirsoft.net/utis/shexview.html	06/10/2007 06:

2254 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

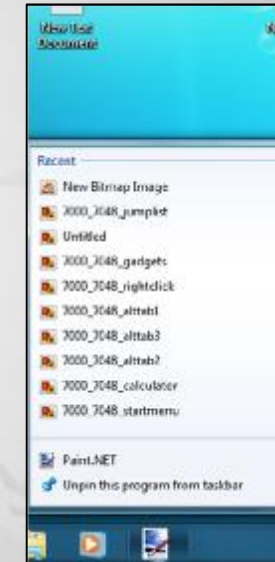
## 윈도우 분석 예제: LNK Parser

바로가기(**Short Cut**)으로 사용자의 원하는 위치에 실행 아이콘을 위치하거나 내 최근 문서, 점프리스트 등에 활용되며 대상 파일에 대한 파일명, 파일 위치, 시간값(**UTC기준**) 등 자세한 정보를 기록하고 있다. 사용자의 의도로 생성 할 수도 있으나, 많은 경우 의도와 상관없이 생성 되고 있다.

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Inhyun\Desktop\lp64.v.0.59.win>lp64.exe "Cannon.001 - Shortcut.lnk"
lp <lnk parser> - limited ver: 0.59; Copyright (c) TZWorks LLC
Licensed for Demo use only.
run time: 11/29/2013 21:39:06 [UTC]
cmdline: lp64.exe "Cannon.001 - Shortcut.lnk"

source path/filename: Cannon.001 - Shortcut.lnk
file modified: 11/29/2013 21:36:10 [UTC]
file accessed: 11/29/2013 21:36:10 [UTC]
file created: 11/29/2013 21:36:10 [UTC]
Target flags: HasLinkTargetIDList, HasLinkInfo, HasRelativePath, HasWorkingDir, IsUnicode, DisableLinkPathTracking
Target attributes: FILE_ATTRIBUTE_ARCHIVE
Target modified: 11/23/2013 18:12:21.368 [UTC]
Target accessed: 11/23/2013 18:09:21.227 [UTC]
Target created: 11/23/2013 18:09:21.227 [UTC]
Target ObjID time: 11/23/2013 16:41:50.375 [UTC]
Parsed size: 0x000001b5 [437 bytes]
Target file size: 0x7c7efe00 [2088697344 bytes]
Show cmd: [SW_SHOWNORMAL]
ID List: Cannon.001
Volume Type: fixed
Volume serial num: beb3-6e10
Volume label: BOOTCAMP
Local base path: C:\Users\Inhyun\Desktop\Cannon.001
Relative path: ..\Cannon.001
Working directory: C:\Users\Inhyun\Desktop
NETBIOS name: bootcamp
Volume ID: 137c9f3c-3c87-499e-84ac-9699cb5d9082
Object ID: 26ac944b-545e-11e3-afce-001c4270c743
MAC address: 00-1c:42:70:c7:43

C:\Users\Inhyun\Desktop\lp64.v.0.59.win>
```



**UTC:** 협정 세계시(국제 협정에 의하여 인위적으로 유지 되고 있는 시각)으로 한국은 UTC 기준 +9:00로 계산

[www.tzworks.net](http://www.tzworks.net)

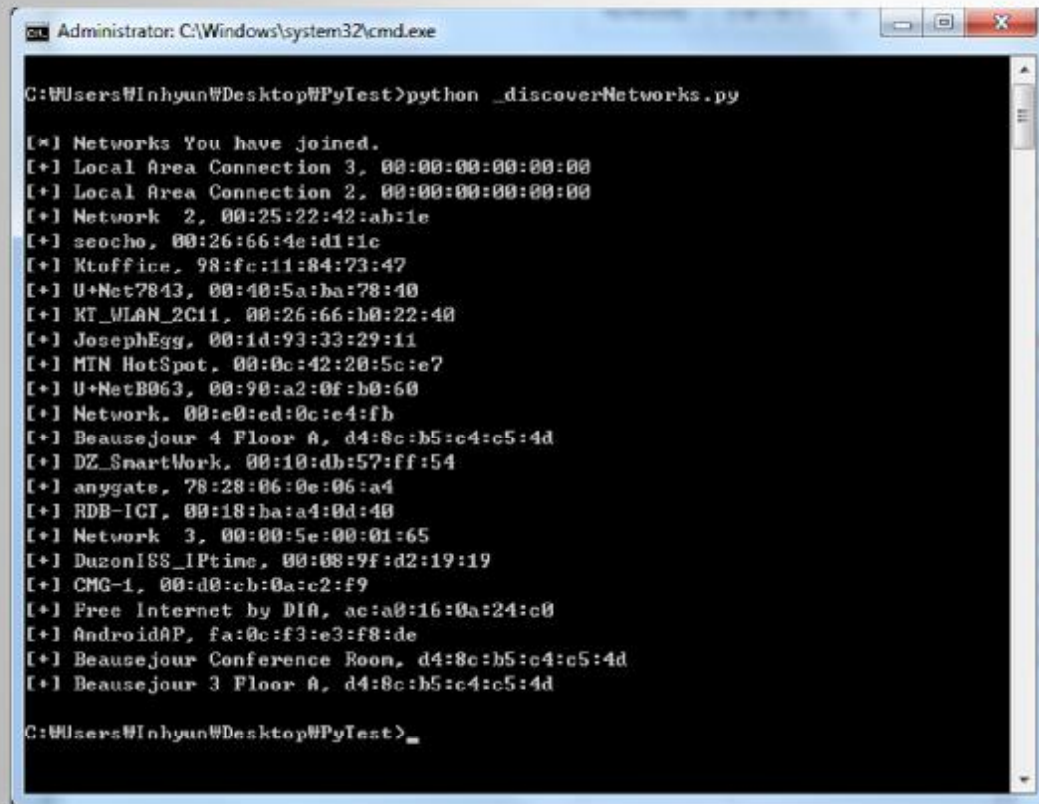
최근 문서 위치

- Windows XP : C:\Documents and Settings\\Recent
- Windows 7 : C:\Users<user name>\AppData\Roaming\Microsoft\Windows\Recent

## 윈도우 분석 예제: Registry

레지스트리(Windows Registry)는 모든 하드웨어, 운영 체제 소프트웨어, 대부분의 비운영 체제 소프트웨어, 사용자 PC 선호도 등에 대한 정보와 설정이 들어 있다.

이전에 윈도 프로그램에 대한 구성 설정을 담는 데에는 각 프로그램마다 INI 파일이 사용 되었으나 시스템 여러 곳에 퍼짐으로써 찾기가 어려운 이유로 윈도 레지스트리가 도입되었다.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Inhyun\Desktop\PyTest>python _discoverNetworks.py

[*] Networks You have joined.
[+] Local Area Connection 3, 00:00:00:00:00:00
[+] Local Area Connection 2, 00:00:00:00:00:00
[+] Network 2, 00:25:22:42:ab:1e
[+] seocho, 00:26:66:4e:d1:1e
[+] Ktoffice, 98:fc:11:84:73:47
[+] U+Net7843, 00:40:5a:ba:78:40
[+] KT_WLAN_2C11, 00:26:66:b0:22:40
[+] JosephEgg, 00:1d:93:33:29:11
[+] MTN HotSpot, 00:0c:42:20:5c:e7
[+] U+NetB063, 00:90:a2:0f:b0:60
[+] Network, 00:e0:ed:0c:e4:fb
[+] Beausejour 4 Floor A, d4:8c:b5:c4:c5:4d
[+] DZ_SmartWork, 00:10:db:57:ff:54
[+] anygate, 78:28:06:0e:06:a4
[+] RDB-ICI, 00:18:ba:a4:0d:40
[+] Network 3, 00:00:5e:00:01:65
[+] DuzonISS_IPtime, 00:08:9f:d2:19:19
[+] CMG-1, 00:d0:cb:0a:c2:f9
[+] Free Internet by DIA, ac:a0:16:0a:24:c0
[+] AndroidAP, fa:0c:f3:e3:f8:de
[+] Beausejour Conference Room, d4:8c:b5:c4:c5:4d
[+] Beausejour 3 Floor A, d4:8c:b5:c4:c5:4d

C:\Users\Inhyun\Desktop\PyTest>
```

파이썬 코드를 이용한 연결되었던 네트워크 정보 확인  
해커의 언어, 치명적 파이썬, TJ 오코너 저/김선국 역



```
_discoverNetworks.py - C:\Users\Inhyun\Desktop\_discoverNetworks.py
File Edit Format Run Options Windows Help

import winreg

def val2addr(val):
    addr = ""
    #print ("val:", val)
    for ch in val:
        #print (str(hex(ch)))
        if (ch<16):
            tenHex = str(hex(ch))[2]
            addr += '0x' + tenHex
        else:
            addr += str(hex(ch))
        #print (addr)
    addr = addr.replace('0x', '').[0:]
    return addr

def printNets():
    net = "SOFTWARE\Microsoft\Windows NT\CurrentVersion+\
        \NetworkList\Signatures\Unmanaged"
    key = winreg.OpenKey(winreg.HKEY_LOCAL_MACHINE, net)
    print ("\n[*] Networks You have joined.")
    for i in range(100):
        try:
            #print (i)
            guid = winreg.EnumKey(key, i)
            netKey = winreg.OpenKey(key, str(guid))
            (n, addr, t) = winreg.EnumValue(netKey, 5)
            (n, name, t) = winreg.EnumValue(netKey, 4)
            macAddr = val2addr(addr)
            macLen = len(macAddr)
            netName = str(name)
            print ('[+] ' + netName + ', ' + macAddr[1:10])
            winreg.CloseKey(netKey)
        except OSError:
            break

def main():
    printNets()


if __name__ == '__main__':
    main()

Ln: 10 Col: 1
```



## 윈도우 분석 예제

“윈도우는 당신의 많은 행위를 기억하고 있다.”



**BoB** 챌린지  
디지털포렌직 챌린지

## BoB 챌린지

### 배경

인터넷의 발달로 사이버 범죄와 불법적인 인터넷 정보가 증가함에 따라 사이버 범죄에 사용되는 기술 또한 비약적인 발전을 거듭하고 있지만, 기존에 발생하는 사이버 범죄에 대한 전문적인 조사/분석할 수 있는 포렌식 전문가가 부족한 실정. 실무형 포렌식 전문가 양성을 통한 정보보안 사업 역량을 강화할 수 있도록 포렌식 교육 콘텐츠를 개발하고, 교육생들을 평가하기 위한 방안 제시.

### 목적

한국정보기술연구원은 IT전문가 양성 및 연구개발, IT국제협력 강화를 중심으로 IT 교육에 대한 선도적인 역할을 수행하고 있습니다. 기존의 부족한 전문 인력을 보완하기 위한 전문 교육 및 평가방안이 필요합니다.

이에 전문 디지털 포렌식을 활용하여 실습할 수 있는 교육 콘텐츠 개발 및 운영/평가할 수 있는 방안을 마련

## BoB 챌린지: 로드맵

**보안 일반** BoB 교육생(수료자 포함) 및 멘토단 대상

**기초 강좌** 포렌식 개요/도구 소개/Artifact 수집 및 분석 등

**자율 학습** 학습된 내용을 복습하고 반복 학습 및 실습을 수행할 수 있는 가이드 제시

**평가** BoB Challenge를 통해 교육생의 학습 능력 평가 및 교육생간의 경쟁심을 통해 집중력을 높이고 관심을 유발

**피드백** 교육자/교육대상/교육기관의 피드백을 통한 차후 보완점 모색

이론 및 실무 능력 배양



# 최근 디지털 포렌식 분석 이슈



## 1. 이직 및 퇴직시점에서의 주요 정보에 대한 유출

60%

이직 및 퇴직대상자에 대한 삭제 파일리스트 및 특정 파일 소지여부 확인  
퇴직 후 동종업계의 회사로 이직 및 창업



## 2. 휴대폰을 통한 자료 유출 및 사생활 침해

20%

HDD분석 중 휴대폰을 외장형저장장치로 사용이력 확인  
타인의 휴대폰 내 주요 자료(통화내역, 사진파일등)를 몰래 백업



## 3. 내부 보안프로그램의 로그를 통한 불법 행위 확인

10%

허가된 자료백업 업무 외 내부 자료 다량 백업  
다양한 보안프로그램 로그를 조합하여 사용자 행위 분석



## 4. 기타. 침해사고, 검증, 코드 분석 등...

10%

침해 사고 분석, 전산 처리 시스템 검증, 분석 보고서 검증  
두 제품의 핵심 소스 코드 유사도 분석

## BoB 챌린지: 디지털 포렌식 챌린지

추가적으로 **BoB(Best of the Best)** 평가를 위한 경쟁 평가 프로그램을 수행할 수 있도록 하며, 본 평가 프로그램은 빙고 형식의 교육 프로그램으로 9가지의 문제에 대한 문제별 난이도가 다르게 측정되어 있으며, 교육생이 각 문제에 대한 빙고 수행 시 추가점을 배점하는 시스템으로 구성

<b>A</b>	<b>B</b>	<b>B</b>
<b>C</b>	<b>C</b>	<b>B</b>
<b>A</b>	<b>B</b>	<b>C</b>

추가 점수 획득

- 총 9문항의 문제는 동시에 공개되지 않음(2문제 > 3문제 > 4문제 등으로 공개)
- 난이도는 C(낮음) < B(보통) < A(높음) 의 순으로 조정
- 각 난이도별 배점이 다르며, 빙고 라인에 따른 가산점 부여  
(예: A-C-C 20점, A-B-B 30점 등)

감사합니다.