

# Forensic Study - 1

## What is the forensic?

---

---

2016.09.20

---

KUICS

---

2014210009 주어진

---

# 목차

---

1. 포렌식?

---

2. 사례

---

3. 무엇을 배울 것인가?

---

부록) GitHub

---

# 포렌식?

컴퓨터 포렌식( 영어: computer forensics, computer forensic science) 또는 컴퓨터 법의학( - 法醫學)은 전자적 증거물 등을 사법기관에 제출하기 위해 데이터를 수집, 분석, 보고서를 작성하는 일련의 작업을 말한다.

과거에 얻을 수 없었던 증거나 단서들을 제공해 준다는 점에서 획기적인 방법이다. 컴퓨터 포렌식은 사이버 해킹 공격, 사이버 범죄시 범죄자들은 컴퓨터, 이메일, IT 기기, 스마트폰 등의 운영체제, 애플리케이션, 메모리 등에 다양한 전자적 증거를 남기게 되면서, 사이버 범죄자 추적 및 조사에 핵심적인 요소가 되고 있다.

출처 : [https://ko.wikipedia.org/wiki/%EC%BB%B4%ED%93%A8%ED%84%B0\\_%ED%8F%AC%EB%A0%8C%EC%8B%9D](https://ko.wikipedia.org/wiki/%EC%BB%B4%ED%93%A8%ED%84%B0_%ED%8F%AC%EB%A0%8C%EC%8B%9D)

# 포렌식?

```

.text:00411690
.text:00411690
.text:00411691
.text:00411693
.text:00411699
.text:0041169A
.text:0041169B
.text:0041169C
.text:004116A2
.text:004116A7
.text:004116AC
.text:004116AE
.text:004116B3
.text:004116B5
.text:004116B8
.text:004116BC
.text:004116C0
.text:004116C4
.text:004116C8
.text:004116CC
.text:004116D0
.text:004116D4
.text:004116D8
.text:004116DC
.text:004116E0
.text:004116E4
.text:004116E8
.text:004116EC
.text:004116F0
.text:004116F4
.text:004116F8
.text:004116FC
.text:00411700
.text:00411702
.text:00411704
.text:00411707
.text:00411708
.text:0041170E
.text:00411710
.text:00411715
.text:00411717
.text:00411718
.text:0041171A
.text:0041171B
.text:00411721
.text:00411726
.text:00411727

        push    ebp
        mov     ebp, esp
        sub     esp, 0E0h
        push    ebx
        push    esi
        push    edi
        lea     edi, [ebp+var_E0]
        mov     ecx, 38h
        mov     eax, 0CCCCCCCCh
        rep stosd
        mov     eax, ___security_cookie
        xor     eax, ebp
        mov     [ebp+var_4], eax
        mov     [ebp+CmdLine], 73h
        mov     [ebp+var_1B], 68h
        mov     [ebp+var_1A], 75h
        mov     [ebp+var_19], 74h
        mov     [ebp+var_18], 64h
        mov     [ebp+var_17], 6Fh
        mov     [ebp+var_16], 77h
        mov     [ebp+var_15], 6Eh
        mov     [ebp+var_14], 20h
        mov     [ebp+var_13], 20h
        mov     [ebp+var_12], 73h
        mov     [ebp+var_11], 20h
        mov     [ebp+var_10], 20h
        mov     [ebp+var_F], 74h
        mov     [ebp+var_E], 20h
        mov     [ebp+var_D], 36h
        mov     [ebp+var_C], 30h
        mov     [ebp+var_B], 0
        mov     esi, esp
        push    0 ; uCmdShow
        lea     eax, [ebp+CmdLine]
        push    eax ; lpCmdLine
        call    ds:WinExec
        cmp     esi, esp
        call    sub_41110E
        xor     eax, eax
        push    edx
        mov     ecx, ebp
        push    eax
        lea     edx, dword_411748
        call    sub_41124E
        pop     eax
        pop     edx

```

# 포렌식?

C:\Users\wakwke\Desktop\Study>volatility\_2.6\_win64\_standalone.exe -f dbC2fba72206f18493fb393b87606f98 --profile=Win7SP1x64 pslist

Volatility Foundation Volatility Framework 2.6

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xffffffff80024c4870	System	4	0	87	575	-----	0	2017-08-13 16:08:39 UTC+0000	
0xffffffff800414c040	smss.exe	240	4	2	30	-----	0	2017-08-13 16:08:39 UTC+0000	
0xffffffff8003d338e0	csrss.exe	328	304	9	678	0	0	2017-08-13 16:08:44 UTC+0000	
0xffffffff8004cb7060	wininit.exe	412	304	3	79	0	0	2017-08-13 16:08:49 UTC+0000	
0xffffffff8004cb6670	csrss.exe	424	404	10	277	1	0	2017-08-13 16:08:49 UTC+0000	
0xffffffff800569f5d0	services.exe	468	412	11	247	0	0	2017-08-13 16:08:49 UTC+0000	
0xffffffff800569d7e0	winlogon.exe	500	404	6	130	1	0	2017-08-13 16:08:50 UTC+0000	
0xffffffff80056ae8b0	lsass.exe	512	412	8	615	0	0	2017-08-13 16:08:51 UTC+0000	
0xffffffff80056b8b10	lsmd.exe	520	412	10	143	0	0	2017-08-13 16:08:51 UTC+0000	
0xffffffff8005728b10	svchost.exe	636	468	13	376	0	0	2017-08-13 16:08:52 UTC+0000	
0xffffffff80057723d0	vmacthlp.exe	696	468	4	56	0	0	2017-08-13 16:08:52 UTC+0000	
0xffffffff8005787b10	svchost.exe	732	468	8	321	0	0	2017-08-13 16:08:52 UTC+0000	
0xffffffff80057e0720	svchost.exe	812	468	23	520	0	0	2017-08-13 16:08:52 UTC+0000	
0xffffffff800586fb10	svchost.exe	864	468	22	452	0	0	2017-08-13 16:08:52 UTC+0000	
0xffffffff8005880870	svchost.exe	912	468	51	1122	0	0	2017-08-13 16:08:53 UTC+0000	
0xffffffff80058bf7e0	audiocd.exe	996	812	7	135	0	0	2017-08-13 16:08:53 UTC+0000	
0xffffffff8005907060	TrustedInstall	352	468	5	217	0	0	2017-08-13 16:08:53 UTC+0000	
0xffffffff8005909b10	svchost.exe	264	468	27	773	0	0	2017-08-13 16:08:53 UTC+0000	
0xffffffff80044ef510	svchost.exe	980	468	21	419	0	0	2017-08-13 16:08:55 UTC+0000	
0xffffffff8005956210	spoolsv.exe	1108	468	14	343	0	0	2017-08-13 16:08:55 UTC+0000	
0xffffffff800595bb10	svchost.exe	1140	468	22	324	0	0	2017-08-13 16:08:55 UTC+0000	
0xffffffff8005b90b10	svchost.exe	1248	468	23	285	0	0	2017-08-13 16:08:56 UTC+0000	
0xffffffff8005bc4060	sppsvc.exe	1300	468	4	150	0	0	2017-08-13 16:08:56 UTC+0000	
0xffffffff8005c07b10	VGAAuthService	1388	468	4	89	0	0	2017-08-13 16:08:56 UTC+0000	
0xffffffff8005b5b520	vmtoolsd.exe	1436	468	10	299	0	0	2017-08-13 16:08:56 UTC+0000	
0xffffffff8005c75710	ManagementAgen	1480	468	11	100	0	0	2017-08-13 16:08:56 UTC+0000	
0xffffffff8005cf42a0	svchost.exe	1720	468	7	98	0	0	2017-08-13 16:08:57 UTC+0000	
0xffffffff8005d77b10	dlhhost.exe	1820	468	22	211	0	0	2017-08-13 16:08:58 UTC+0000	
0xffffffff8003e8e060	WmiPrvSE.exe	1892	636	10	201	0	0	2017-08-13 16:08:58 UTC+0000	
0xffffffff8003f9c060	dlhhost.exe	1960	468	19	213	0	0	2017-08-13 16:08:58 UTC+0000	
0xffffffff80044ab060	msdtc.exe	1076	468	15	158	0	0	2017-08-13 16:08:59 UTC+0000	
0xffffffff800451f060	VSSVC.exe	2080	468	7	123	0	0	2017-08-13 16:09:00 UTC+0000	
0xffffffff8004cfd060	mscorsvw.exe	2496	468	9	156	0	1	2017-08-13 16:09:09 UTC+0000	
0xffffffff8004d93b10	mscorsvw.exe	2520	468	6	101	0	0	2017-08-13 16:09:09 UTC+0000	
0xffffffff8004dad620	taskhost.exe	2624	468	10	184	1	0	2017-08-13 16:09:12 UTC+0000	
0xffffffff8004de5b10	dwm.exe	2704	884	4	77	1	0	2017-08-13 16:09:12 UTC+0000	
0xffffffff8004defb10	explorer.exe	2732	2664	34	899	1	0	2017-08-13 16:09:12 UTC+0000	
0xffffffff80056b4500	SearchIndexer	2988	468	15	750	0	0	2017-08-13 16:09:15 UTC+0000	
0xffffffff80057c9720	SearchProtocol	1788	2988	7	285	0	0	2017-08-13 16:09:15 UTC+0000	
0xffffffff8005850b10	SearchFilterHo	2148	2988	5	107	0	0	2017-08-13 16:09:15 UTC+0000	
0xffffffff8005874b10	vmtoolsd.exe	2236	2732	7	176	1	0	2017-08-13 16:09:17 UTC+0000	
0xffffffff80044d4730	WmiPrvSE.exe	2348	636	13	305	0	0	2017-08-13 16:09:19 UTC+0000	
0xffffffff80049bb060	WmiApSrv.exe	2408	468	7	122	0	0	2017-08-13 16:09:21 UTC+0000	
0xffffffff8004b5e580	vmtoolsd.exe	2900	468	12	219	0	0	2017-08-13 16:09:24 UTC+0000	

# 포렌식 - 사례

<http://www.jejusori.net/?mod=news&act=articleView&idxno=168929>

## 제주의소리

### 제주서 아내 죽인 40대 징역 30년 선고후 '오열'

설득 끝에 부검이 이뤄지면서 경찰은 남편을 용의자로 의심하기 시작했다. 목 졸림에 의한 살인이라는 부검의의 소견이 나왔기 때문이다. 부인의 몸에서는 수면제 성분도 나왔다.

신고 당시 집안에는 남편과 자녀들만 있었고 외부 침입 흔적은 없었다. 경찰은 고씨가 신고 전날인 10일 밤 11시부터 이튿날 오후 2시 사이 부인을 살해한 것으로 추정했다.

시건을 넘겨받은 검찰은 1차 부검과정에서 확보한 자료를 다른 부검의에게도 의뢰해 교차 확인을 벌였다. 그 결과 1차와 같이 외부적 목 졸림에 의한 사망이라는 소견이 나왔다.

남편이 범행을 계속 부인하자 동선수사를 통해 고씨의 범행을 입증할 만한 자료를 확보했다. 고씨의 컴퓨터와 휴대전화에서 '보험금', '사망', '부검' 등을 검색한 흔적이 다수 나왔다.

2~3월 기록된 검색어는 '집에서 죽으면 처리하는 법', '사망시 119 부르지 않는 법', '뒤로 넘어지면서 화장실에서 사망', '사망시 연금 수령', '살해시 보험금' 등 매우 구체적이었다.

검찰 조사에서는 고씨가 도박 빚에 시달리고 있었고 1년 전 아내 이름으로 1억원의 보험에 가입된 사실이 드러났다.



# 포렌식 - 사례

<http://www.law.go.kr/precInfoP.do?precSeq=69360>

판례정보

신뢰할 수 있는 법제처  
국가법령정보센터

판시사항 | 판결요지 | 참조조문 | 참조판례 | 전문 | 관련자료 | **판례체계도**

법령용어 | 화면내검색 |   

2001도4392 판결 등 참조).

원심은, 적법하게 채택한 판시 증거들을 종합하여 인정되는 여러 간접사실, 즉 ① 피고인이 범행을 은폐하기 위하여 선택한 방법은 피해자의 사체를 80여 조각으로 훼손하여 살점을 잘라 끊이고 믹서에 갈고 사체를 찾지 못하게 하기 위해 10여 곳 이상의 장소에 유기한 것인바, 이는 경험칙상 피해자를 살해한 자가 자신의 범행을 은폐하기 위한 것일 가능성이 높은 점, ② 피고인은 피해자가 사망한 것으로 추정되는 시점에서 불과 30분에서 1시간 정도밖에 되지 않았는데 범행은닉의 방법에 대하여 고민이나 갈등을 하지 않고 피해자를 화장실로 옮겨 곧바로 과도를 솥돌로 갈면서 피해자의 동맥을 잘라 피를 빼려고 하였고, 범행 후 사체손괴 과정과 손괴한 사체와 피해자의 유품을 서울역, 야산, 부대주변 인근 아파트 등에 치밀하고 신속하게 유기하였으며, 범행을 은폐하기 위하여 범행 직후 인터넷을 검색하여 관련 정보를 검색하고 피해자의 행적을 조작한 점, ③ 피해자의 머리 뒤통수 부위 상해는 바닥에 부딪히거나 도구에 의한 물리력이 가해진 경우 발생할 수 있는 상처이고, 이로 인해 출혈이 계속된 흔적이 있어 생전에 발생한 것이며, 피해자의 이빨이 하늘로 켜진 것은 손가락을 넣었다 단순히 잡아당기는 힘에 의해서는 생기기 어려우므로, 피해자가 유형력의 행사에 의해서 사망한 것은 아니라고 하더라도 생전에 일정한 유형력의 행사에 의하여 상해를 입었다고 볼 수 있는 점, ④ 피고인은 피해자와 2004년 말경부터 알고 지냈으며 서로 간에 결혼을 생각하며 교제를 하는 사이였으나 피고인은 피해자의 피부문제 등으로 관계를 청산하려고 하였으며 평소에도 피해자에게 심한 욕설을 하였을 뿐 아니라 피해자를 짜증스럽게 생각하여 피고인이 피해자와 다투는 과정에서 피해자를 살해할 충분한 동기가 있는 점 등을 종합하여, 피고인이 불상의 방법으로 피해자를 살해한 뒤 자신의 범행을 은폐하기 위해 사체를 80여 조각으로 손괴하여 유기한 것으로 볼 수 있어 작위에 의한 살인죄를 인정할 수 있다고 판단하였다. 또한, 원심은 '피해자가 자살하기 위해

---

# 무엇을 배울 것인가?

1. Windows Dump Analysis
2. Windows Registry Analysis
3. etc.



# 무엇을 배울 것인가?

## 1. Windows Dump Analysis

- Windows의 메모리 구조, DLL이란 무엇인가등의 지식이 필요.

## 2. Windows Registry Analysis

- Windows Registry의 구조에 대한 지식이 필요.

## 3. etc.

- image나 PDF등등...

# GitHub

<https://github.com/>

[Features](#)[Business](#)[Explore](#)[Marketplace](#)[Pricing](#)[Sign in](#) or [Sign up](#)

## Built for developers

GitHub is a development platform inspired by the way you work. From **open source** to **business**, you can host and review code, manage projects, and build software alongside millions of other developers.

Username

Email

Password

Use at least one letter, one numeral, and seven characters.

[Sign up for GitHub](#)

By clicking "Sign up for GitHub", you agree to our [terms of service](#) and [privacy policy](#). We'll occasionally send you account related emails.

---

# GitHub

참고 : <https://nolboo.kim/blog/2013/10/06/github-for-beginner/>

# GitHub

<https://desktop.github.com/>



[Overview](#) [Release Notes](#) [Help](#)

## The new native

Extend your GitHub workflow beyond your browser with GitHub Desktop, completely redesigned with Electron. Get a unified cross-platform experience that's completely open source and ready to customize.

[Download for Windows \(64bit\)](#)

Download for [macOS](#) or [Windows \(msi\)](#)

By downloading, you agree to the [Terms and Conditions](#).

# GitHub

[https://github.com/akwkek11/KUICS\\_Study\\_Forensic](https://github.com/akwkek11/KUICS_Study_Forensic)

3 commits

1 branch

0 releases

1 contributor

Branch: master [New pull request](#) [Find file](#) [Clone or download](#)

akwkek11 Add Directories

1. What is Forensic	Add Directories	
2. OS - Theory	Add Directories	
3. Windows Theory (1)	Add Directories	
4. Windows Dump Analysis (1)	Add Directories	
5. Windows Dump Analysis (2)	Add Directories	
6. Windows Registry (1)	Add Directories	7 days ago
7. Windows Registry (2)	Add Directories	7 days ago
8. Windows Registry (3)	Add Directories	7 days ago
9. Windows Theory (2)	Add Directories	7 days ago
.gitattributes	Added .gitattributes & .gitignore files	7 days ago
.gitignore	Added .gitattributes & .gitignore files	7 days ago
README.md	Add Directories	7 days ago

Clone with HTTPS ⓘ

Use Git or checkout with SVN using the web URL.

[https://github.com/akwkek11/KUICS\\_Study\\_Fo](https://github.com/akwkek11/KUICS_Study_Fo)

[Open in Desktop](#) [Download ZIP](#)

Clone akwkek11/KUICS\_Study\_Forensic to your computer and use it in GitHub Desktop.

# GitHub

[https://github.com/akwkek11/KUICS\\_Study\\_Forensic](https://github.com/akwkek11/KUICS_Study_Forensic)

The screenshot displays the GitHub web interface for a repository. At the top, there are tabs for 'Changes' and 'History', with 'History' being the active tab. To the right of these tabs is a 'Pull request' button and a settings gear icon. Below the tabs is a dark horizontal bar representing the commit history timeline, with a 'Sync' button on the right. A tooltip points to the timeline, stating: 'Pull changes from and push local changes on master to the remote'. Below the timeline, the 'Add Directories' section is visible, showing a list of directories with their respective commit hashes and a green plus icon for each. The directories are:

- 1. What is Forensic#README.md
- 2. OS - Theory#README.md
- 3. Windows Theory (1)#README.md
- 4. Windows Dump Analysis (1)#README.md
- 5. Windows Dump Analysis (2)#README.md

At the bottom of the 'Add Directories' section, there are links for 'GitHub', 'Revert', and 'Expand all'.

# 감사합니다

---

10/8까지는 스터디가 없습니다.

- 9/25~30 : 스터디장의 일본여행
- 10/1~9 : 연휴

과제 : GitHub 설치 후 Clone까지!