Chapter 2. Essential Technical Concepts

필수적인 기술 개념~

융합보안학과 윤세영

유투브 주소:
https://youtu.be/i_EkD127uVo

서론

- 디지털 포렌식 조사를 수행하기 전에~~~ 컴퓨팅의 주요 기술 개념들을 이해하고 있어야 함
- 컴퓨터에 정보가 어떻게 저장되는지, 디지털 파일이 어떻게 구성되는지 등을 자세히 알아야 함

구성

In this chapter, we will cover the following:

- Different number system
- Encoding schema
- File carving and structure
- File metadata
- Hash analysis
- System memory
- Storage
- Filesystem
- Cloud computing
- Windows OS
- Networking

- Decimal (Base-10)
- Binary
- Hexadecimal (Base-16,Base-64)
- Character encoding schema
- File carving
- File structure
- Digital file metadata
- Timestamps decoder
- Hash analysis
- Calculate file hash
- System memory
- Types of computer memory storage
- Primary storage
- RAM
- ROM
- Secondary storage
- Backup storage
- HDD
- Hard disk storage
- SSD
- DCO and HPA
- Considerations for data recovery
- File system
- NTFS
- FAT
- Environment for computing
- Cloud computing
- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)
- Windows versions
- Internet protocol (IP) address
- Getting an IP address

Decimal (Base-10)

- Decimal (Base-10) : 10진수
  - 어떤 숫자가 나타내는 값은 10진수에서 그 숫자가 위치한 자릿수에 의해 결정되며, 각 자릿수는 해당 위치에 해당하는 10의 거듭제곱을 곱해 계산됨

$$7{,}654 = 7{,}000 + 600 + 50 + 4$$

Binary

- Binary : 2진수

  - 1과 0으로 표현되는 2진수(base-2) 체계, 컴퓨터에서는 데이터를 이진 형식으로 저장함
  - 0과 1, 두 가지 기호만을 사용하며 2의 거듭제곱을 기준으로 값을 계산
  - 각 1 또는 0은 '비트(bit)', 8비트가 모이면 '바이트(byte)'라고 함

최상위 비트 →

MSB	Binary Digit							LSB
2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
256	128	64	32	16	8	4	2	1

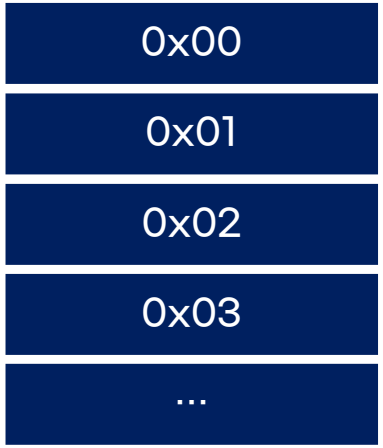
← 최하위 비트

Binary								
1	1	0	0	1	1	0	0	1
Decimal								
1×2^8	1×2^7	0×2^6	0×2^5	1×2^4	1×2^3	0×2^2	0×2^1	1×2^0
256	128	0	0	16	8	0	0	1
= 256+128+0+0+16+8+0+0+1								
= 409								

← 계산 방향

Hexadecimal (Base-16)

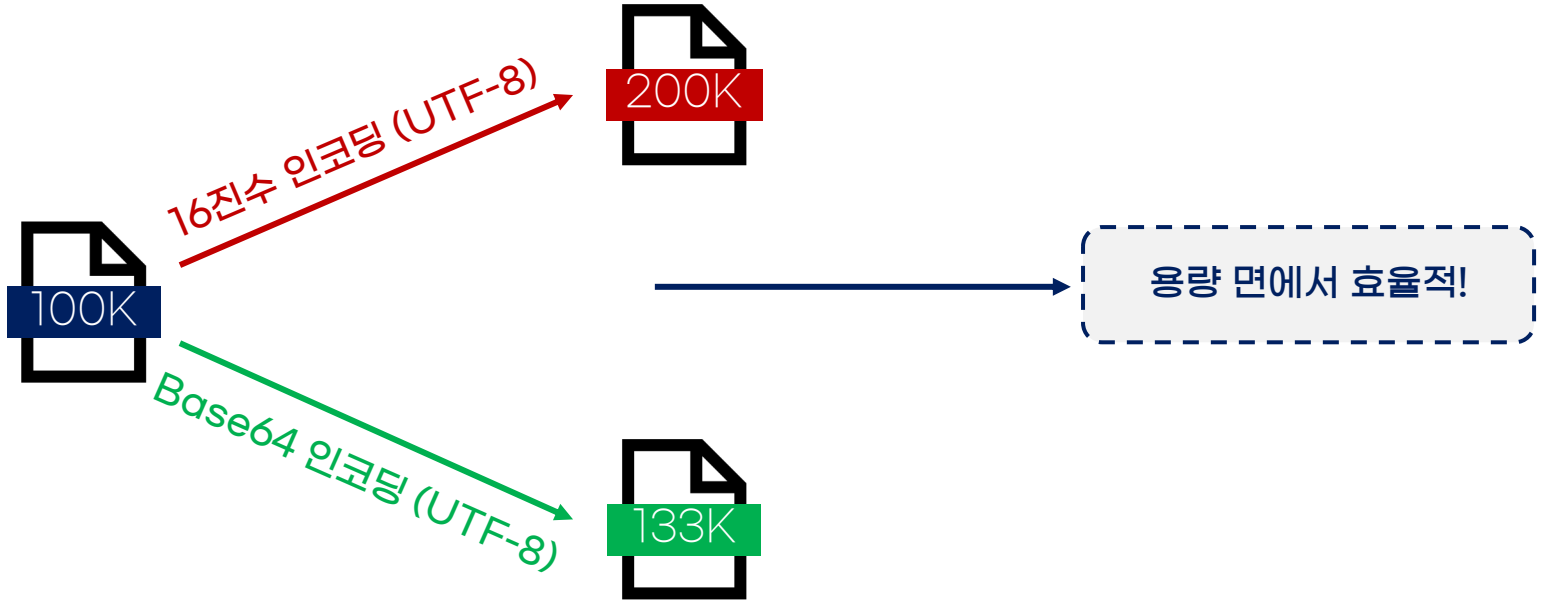
- Hexadecimal (Base-16) : 16진수
  - 16개의 숫자와 기호로 표현
  - 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F
  - 메모리 주소를 확인할 때 주로 사용됨



Hexadecimal (Base-64)

- Hexadecimal (Base-64)

  - 이전 슬라이드의 16진수(hex)와는 바이트가 표현되는 방식에서 차이가 있음
  - 16진수는 바이트마다 두 글자가 필요하지만, Base64는 3바이트당 4글자가 필요함 (더 효율적임)
  - Base64 디코딩 시 개행 문자나 공백 문자는 무시됨



Character encoding schema

- 컴퓨터 내부에서 처리되는 이진 정보를 사람이 읽을 수 있는 텍스트로 변환하는 과정

→ 컴퓨터는 Character encoding schema를 사용하여 0과 1을 A, B, X, Y 등의 문자로 변환함

[컴퓨터가 텍스트를 표현하기 위해 사용하는 주요 encoding schema 두 가지]

- ASCII (American Standard Code for Information Interchange) : https://ascii.cl
- 유니코드(Unicode) : https://unicode.org

ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol
0	0	NUL	16	10	DLE	32	20	(space)	48	30	0
1	1	SOH	17	11	DC1	33	21	!	49	31	1
2	2	STX	18	12	DC2	34	22	"	50	32	2
3	3	ETX	19	13	DC3	35	23	#	51	33	3
4	4	EOT	20	14	DC4	36	24	$	52	34	4
5	5	ENQ	21	15	NAK	37	25	%	53	35	5
6	6	ACK	22	16	SYN	38	26	&	54	36	6
7	7	BEL	23	17	ETB	39	27	'	55	37	7
8	8	BS	24	18	CAN	40	28	(	56	38	8
9	9	TAB	25	19	EM	41	29	)	57	39	9
10	A	LF	26	1A	SUB	42	2A	*	58	3A	:
11	B	VT	27	1B	ESC	43	2B	+	59	3B	;
12	C	FF	28	1C	FS	44	2C	,	60	3C	<
13	D	CR	29	1D	GS	45	2D	-	61	3D	=
14	E	SO	30	1E	RS	46	2E	.	62	3E	>
15	F	SI	31	1F	US	47	2F	/	63	3F	?

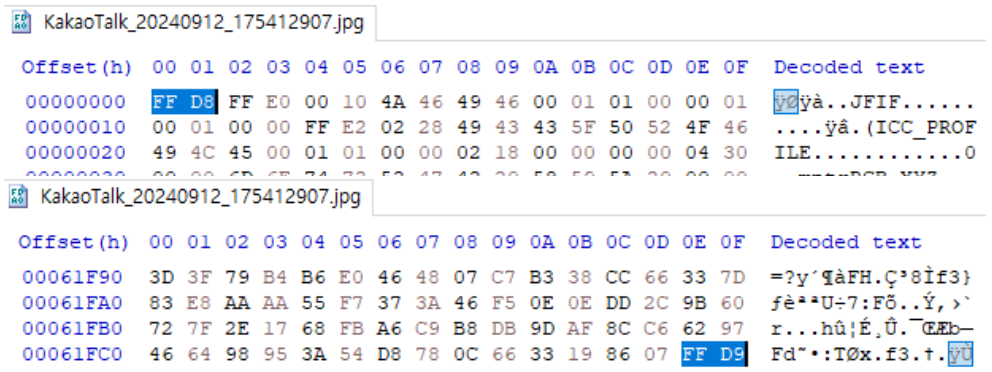
File carving

[파일 카빙] :

비할당 영역: 파일 테이블과 같은 파일 시스템 구조상 더이상 파일 정보가 존재하지 않는 것으로 표시된 디스크 영역

- 저장 매체의 비할당 영역에서 이전에 저장되어 있었던 파일을 복구하는 기법
- 파일 시스템의 파일 메타데이터에 의존하지 않기 때문에 파일 시스템이 존재하지 않거나 고장이 난 경우에도 파일 복구가 가능함 → 파일 내부 구조(헤더·푸터 시그니처 등)를 활용해 실제 데이터를 재조립

SOI (Start Of Image)

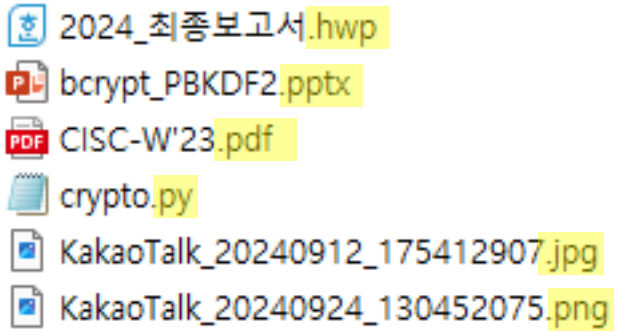


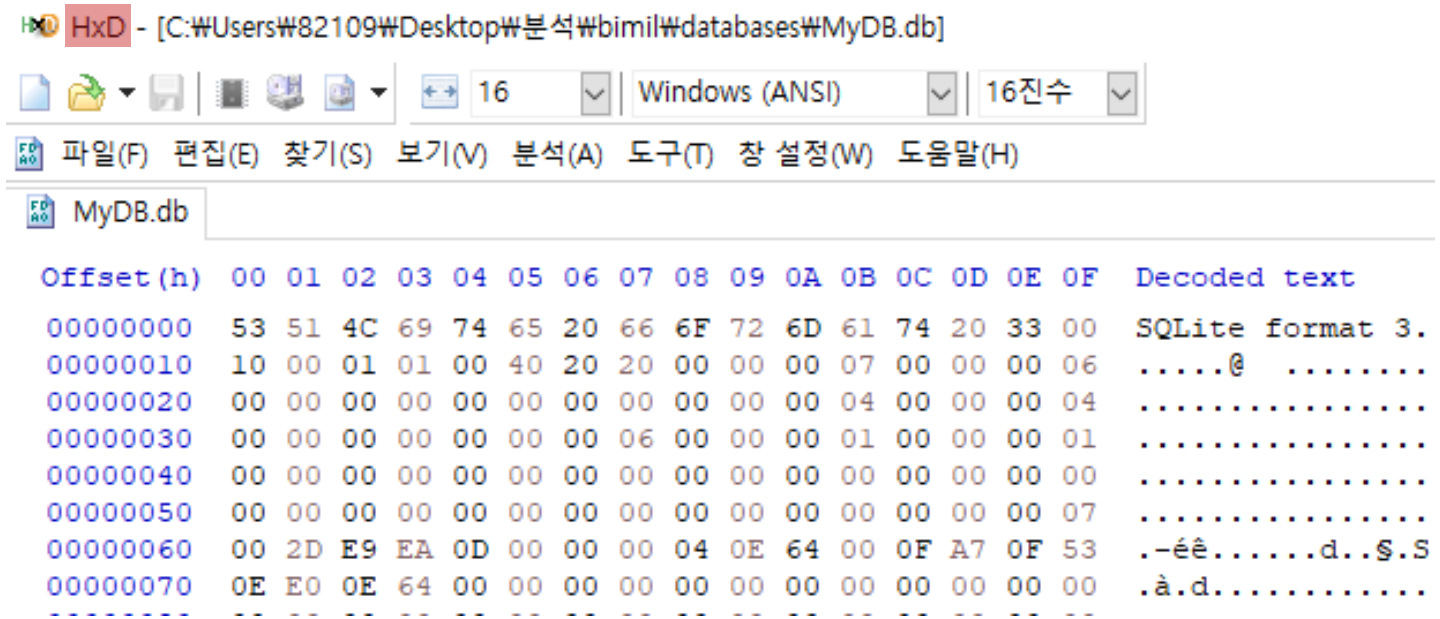
EOI (End Of Image)

File Type	Header Signature (Hex)	Footer Signature (Hex)
JPEG	FF D8 FF E0 FF D8 FF E8	FF D9
GIF	47 49 46 38 37 61 47 49 46 38 39 61	00 3B
PNG	89 50 4E 47 0D 0A 1A 0A	49 45 4E 44 AE 42 60 82
PDF	25 50 44 46 2D 31 2E	25 25 45 4F 46
ZIP	50 4B 03 04	50 4B 05 06
ALZ	41 4C 5A 01	43 4C 5A 02
RAR	52 61 72 21 1A 07	3D 7B 00 40 07 00

File structure

- 파일 확장자(예: .docx, .xls)를 통해 해당 파일 형식을 인식할 수 있음
- 그러나 확장자를 변조하여 실제 파일 형식을 숨길 수 있음 → 파일의 시그니처를 확인!
- HexEditor 를 통해 파일의 형식 및 구조를 확인해 볼 수 있음





Digital file metadata

- 해당하는 파일에 대한 정보를 담고 있음
- ex: 파일 생성 일시, 작성자 이름, 컴퓨터 이름, 용량 등

- 메타데이터에 연결된 정보를 활용해 파일 작성자를 추적하거나 유용한 정보를 획득할 수 있음

윈도우 운영체제

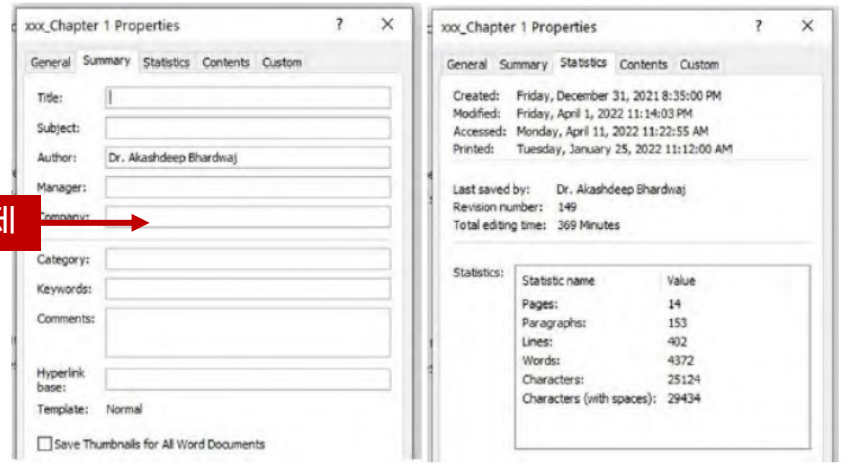
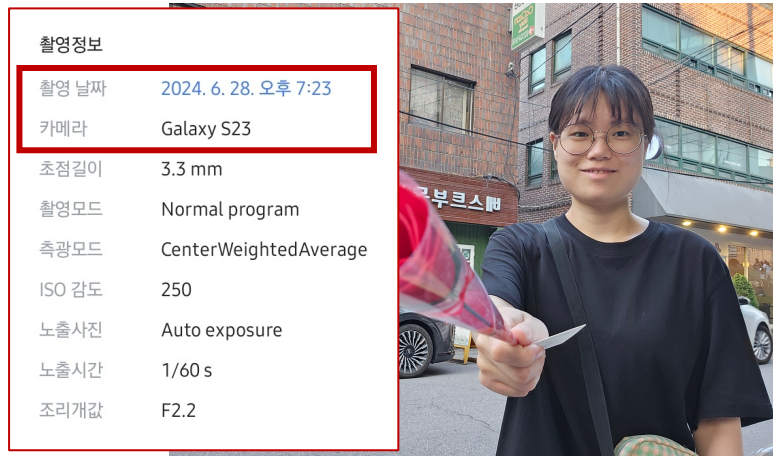


Figure 2.4: *Word file summary and statistics properties*

Mac 운영체제



Digital file metadata

디지털 파일의 메타데이터를 확인하고 편집할 수 있는 무료 도구들

- ExifTool by Phil Harvey (www.sno.phy.queensu.ca/~phil/exiftool)
- Exif Pilot (www.colorpilot.com/exif.html)
- GIMP (www.gimp.org)
- Pdf Metadata Editor (http://broken-by.me/pdf-metadataeditor)
- Mp3tag (www.mp3tag.de/en)
- XnView (www.xnview.com/en/)
- MediaInfo (https://mediaarea.net/en/MediaInfo)

Timestamps decoder

- '타임스탬프' 란 파일과 관련된 날짜 및 시간 정보를 말함
- (마지막으로 액세스한 날짜 및 시간, 마지막으로 업데이트된 날짜, 생성된 날짜 등)

- Microsoft Office 2010부터 2016까지는 그림과 같이 타임스탬프를 포함한 메타데이터를 확인할 수 있음

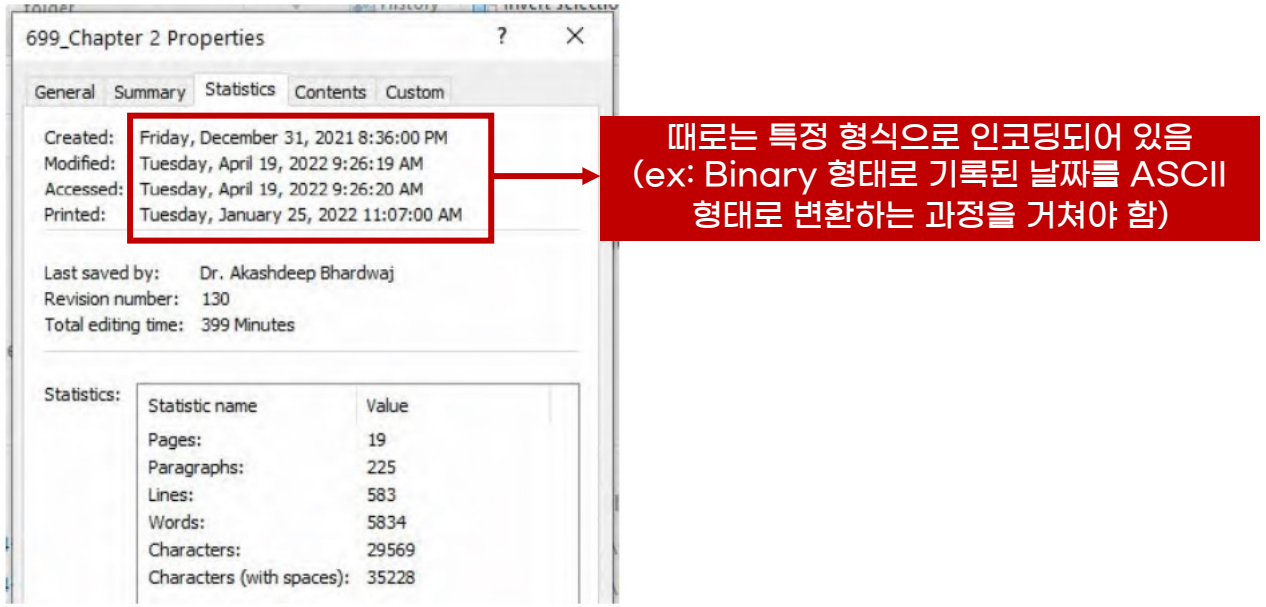


Figure 2.6: *File properties*

Hash analysis

- 조사 과정에서 확보한 모든 디지털 증거의 해시 값을 계산하여 데이터가 변조되지 않았음을 입증해야 함
- 디지털 지문(digital fingerprinting)이라고도 불림
- 디지털 포렌식 조사 시 최초 한 번(분석에 앞서 확보한 포렌식 이미지를 식별하고, 동일한 복제본을 만들기 위해) 과, 조사 종료 후 한 번(데이터 및 포렌식 처리의 무결성을 확인하기 위해) 총 두 번 진행됨

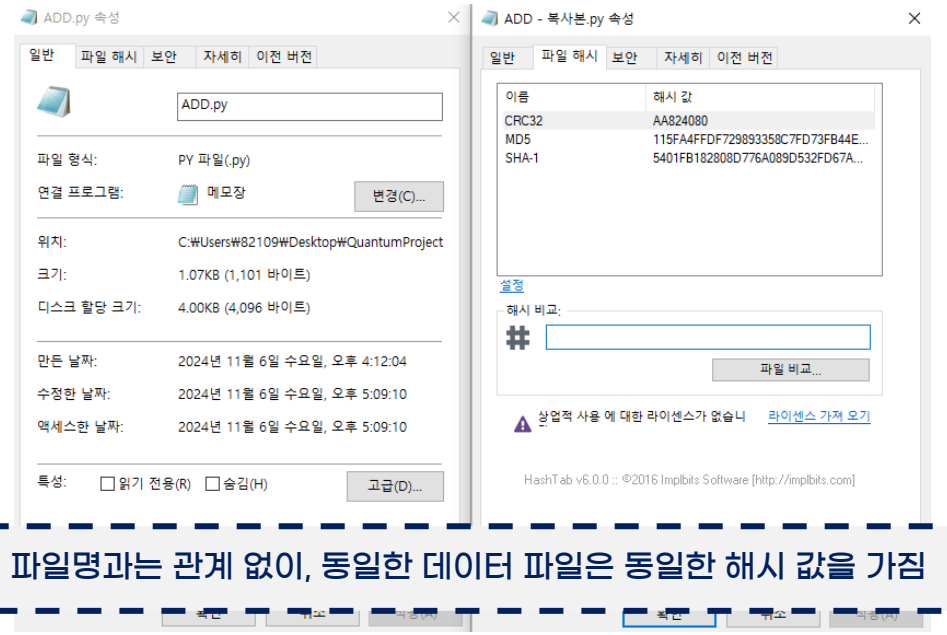
HelloWord

Hello Word

- 해싱은 디지털 파일(입력값)을 고정된 문자열 값(출력값)으로 변환하는 과정
- 해시 값은 고유하며 다른 파일이나 데이터로는 동일한 값을 만들 수 없음

MD5 해시: 04b6f86d49716af8d4f2edf01a309fc8

MD5 해시: ed0a96e83ab7b0910fcbcc131b2e6b82



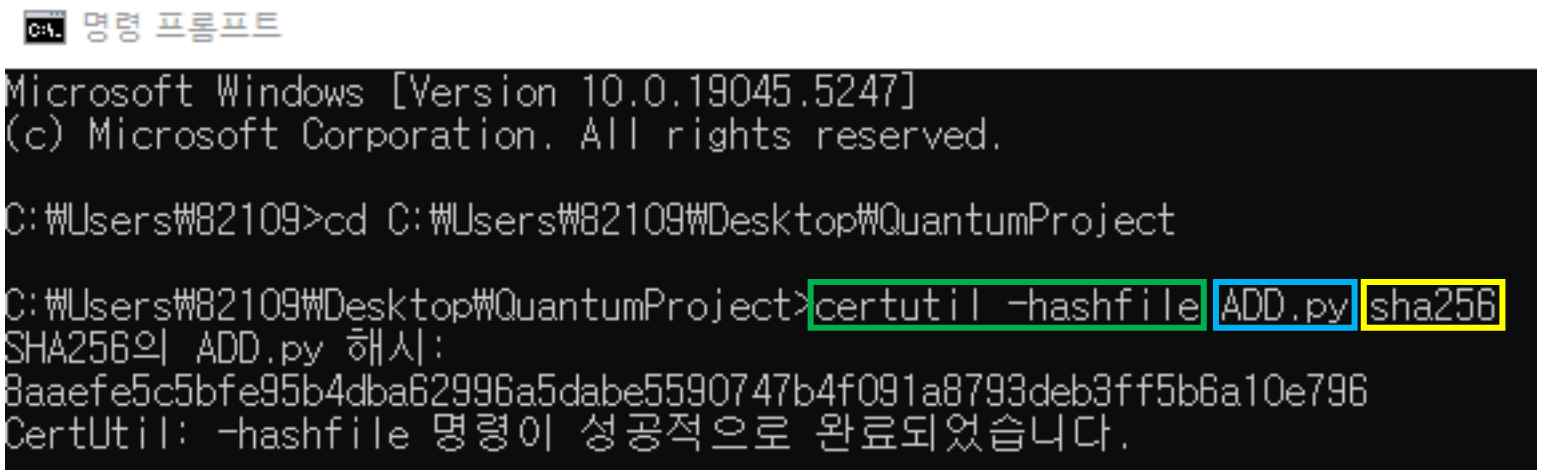
- 파일명과는 관계 없이, 동일한 데이터 파일은 동일한 해시 값을 가짐

Calculate file hash

- 모든 디지털 포렌식 도구에는 해싱 기능이 포함되어 있으나, Windows 운영체제의 기본 해싱 도구나 외부 도구를 사용할 수도 있음

[외부 도구]
- Febooti Hash and CRC : www.febooti.com
- HashMyFile : http://www.nirsoft.net/utils/hashmyfiles.html

[Windows 기본 해싱 기능 사용]
- certutil -hashfile "파일명" "해시알고리즘"



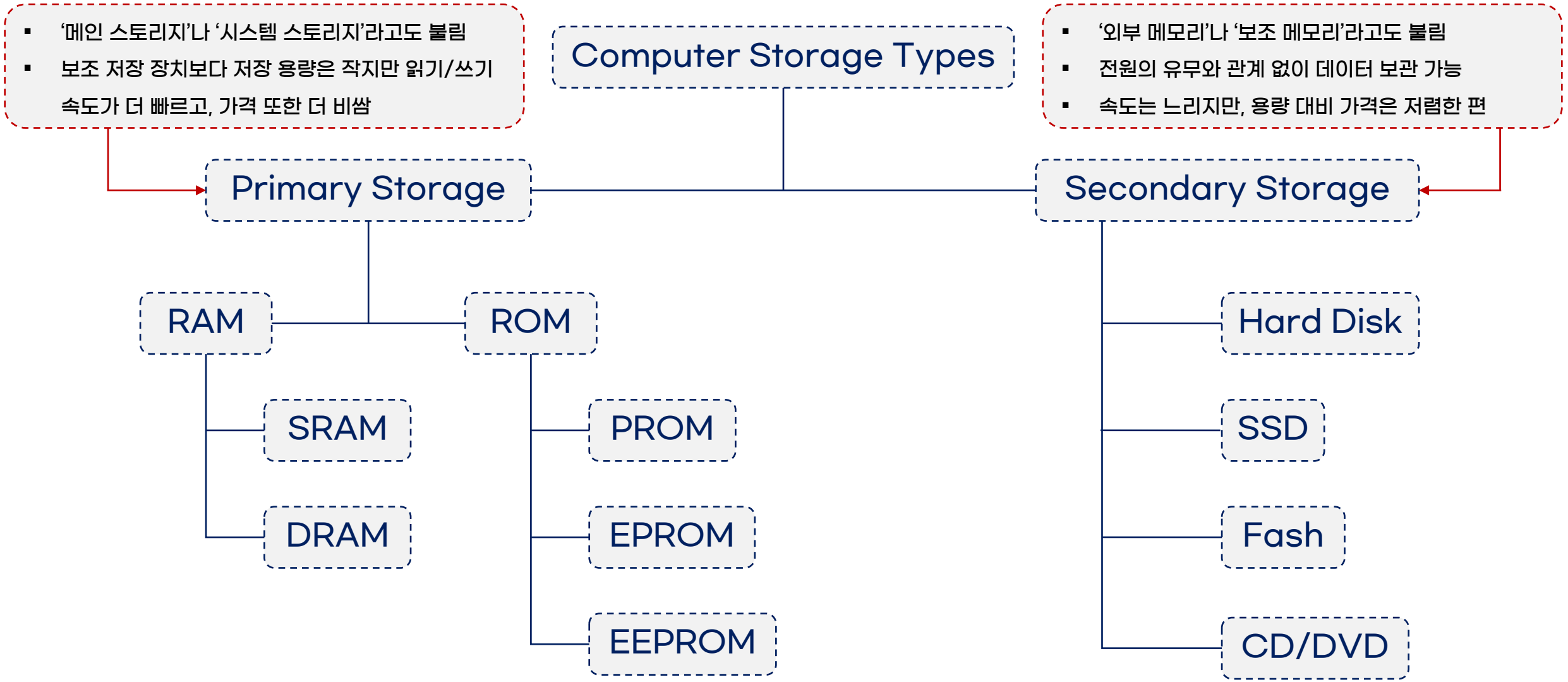
System memory

- 메모리는 컴퓨터에서 즉시 사용하거나 나중에 사용할 데이터를 저장하는 물리적 구성 요소를 의미
- 저장된 정보를 얼마나 오래 유지하느냐에 따라 크게 두 가지 유형으로 구분할 수 있음

[휘발성 메모리(Volatile memory)]
- 데이터를 일정 기간 동안만 저장
- 데이터를 유지하기 위한 전력이 필요
- 전원이 꺼지면 데이터를 잃게 됨
- RAM

[비휘발성 메모리(Non-volatile memory)]
- 전원이 꺼져 있어도 오랫동안 데이터를 보관할 수 있음
- 장기 저장 목적으로 사용
- 컴퓨터 하드 드라이브, 플래시 메모리, ROM(읽기 전용 메모리) 등

Types of computer memory storage



Primary Storage - RAM

- RAM (Random Access Memory)
- 컴퓨터가 데이터를 임시로 저장하고 빠르게 접근하기 위해 사용하는 기억장치
- 다양한 정보가 저장되므로, 디지털 포렌식 관점에서 중요한 장치임

→ 실행 가능한 애플리케이션, 네트워크 세션, 웹 브라우저 기록, 인스턴트 메신저 대화, 비밀번호, 사진, 복호화된 파일 등이 포함

[플립플롭(flip-flop)]
- 내부가 논리 회로이므로 충전 및 방전 대기 시간이 없음
- 기억된 내용을 읽어도 지워지지 않음(비파괴 읽기)
- 리프레시(refresh)가 필요 없어서 안정적이나, 회로가 복잡하여 대규모로 만들면 비용이 비싸짐
- (1비트를 저장-기억하기 위해 여러 개의 트랜지스터 필요)
- CPU 캐시나 레지스터처럼 적은 용량이지만 아주 빠른 속도가 필요한 곳에 주로 사용됨

[커패시터(capacitor)]
- 축전기에 전하를 저장하여, 저렴하게 대용량 메모리를 구성할 수 있음
- (1비트를 저장-기억하기 위해 1개의 트랜지스터와 1개의 커패시터만 있으면 됨)
- 충전 및 방전 시간이 있고, 주기적인 리프레시가 필요함
- 읽을 때 내용이 소모되거나 영향을 줄 수 있음
- 주기억장치(메인 메모리)처럼 큰 용량이 필요한 곳에 주로 사용함

	SRAM (Static RAM)	DRAM (Dynamic RAM)
구조적 특징	플립플롭 (flip-flop)	커패시터 (capacitor)
속도	빠르다	(비교적) 느리다
용량	적다	많다
가격	비싸다	(비교적) 싸다

Primary Storage - ROM

- ROM (Read Only Memory)
- 읽기 작업에만 사용되는 메모리 (쓰기 작업은 지원하지 않음)
- 전원이 꺼져도 저장된 정보를 계속 보존하는 비휘발성 메모리

	PROM	EPROM	EEPROM
Full Name	Programmable Read-Only Memory	Erasable & PROM	Electrically Erasable & PROM
정의	사용자가 한 번만 기록(수정)할 수 있는 ROM	지울 수 있고 다시 사용할 수 있는 프로그래밍 가능 ROM	일반 전압(전기 신호)로 여러 번 지우고 다시 프로그래밍 가능한 ROM
재프로그래밍 가능 횟수	**불가능**	가능 (자외선으로 **전체 삭제 후** 다시 기록)	가능 (**필요한 부분만 선택적으로 삭제**/기록)
(데이터를) 지우는 방법	없음	자외선(UV)으로 전체를 지운 뒤 재프로그래밍 가능	전기적 방식으로 필요한 부분을 선택적으로 지우고 재프로그래밍 가능

Secondary Storage - HDD

- HDD(Hard Disc Drive)
- 데이터가 영구적으로 저장되는 비휘발성 저장 장치
- 자기 저장(magnetic storage) 기술을 사용하여 데이터를 보관함
- 컴퓨터 내부에 장착되어 있는 형태와 외부로 분리(ex: USB)되어 있는 형태가 있음

[플래터(Platter)]

- 알루미늄·유리·세라믹 재질의 원형 디스크로, 데이터가 실제로 기록되는 곳
- 각 플래터는 여러 트랙(track)으로 구성되고, 트랙은 다시 섹터(sector)로 세분화됨
- 보통 500GB 미만의 HDD는 플래터 1개를, 대용량 HDD는 최대 5개의 플래터를 가지고 있음

HDD의 최소 기록 단위
2010년대를 기점으로 대용량 HDD는
섹터당 4096바이트를 기록함

[파티셔닝(Partitioning)]

- 물리적으로 하나인 디스크를 논리적으로 여러 개처럼 나누어 쓰는 기법
- (FAT, NTFS 등 다른 파일 시스템 사용 가능)

Secondary Storage - HDD

[섹터(Sector)]

- 디스크가 실제로 입출력(IO)을 하는 최소 물리 단위 (일반적으로 1섹터 = 512byte)
- 디스크 입출력은 항상 섹터 단위로 이뤄짐

[클러스터(Cluster)]

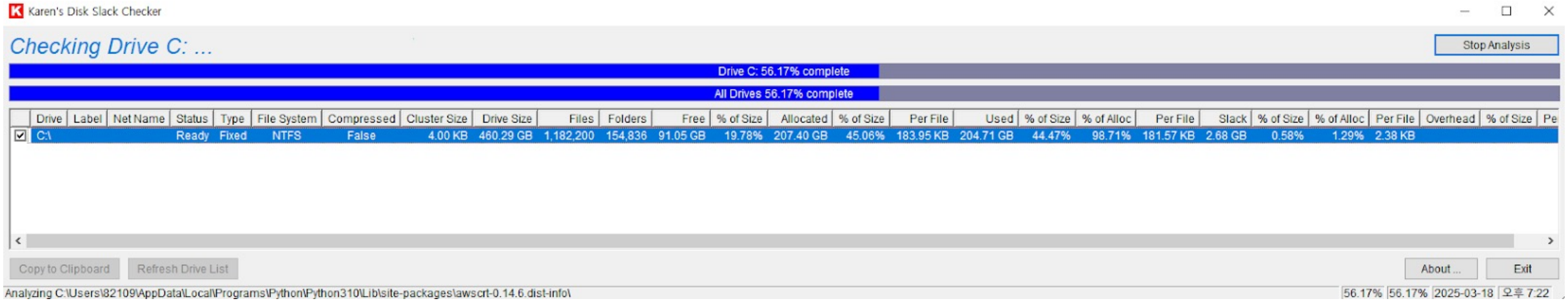
- 운영체제(OS)와 파일시스템이 디스크에 접근할 때 사용하는 최소 논리 단위
- 파일시스템은 입출력 횟수를 줄이기 위해 여러 섹터를 묶어 클러스터로 관리
- 파일시스템 입출력은 항상 클러스터 단위로 이뤄짐

[슬랙 스페이스 (Slack Space)]

- 저장매체의 물리적인 구조와 논리적인 구조의 차이로 발생하는 (낭비) 공간을 의미함

→ 물리적으로는 존재하지만, 논리적으로는 사용할 수 없는 공간임

- 슬랙 스페이스에는 의도적으로 데이터를 숨기거나, 과거에 삭제된 파일이 남아 있을 수 있음



[Disk Slack Checker] 도구를 사용하여 하드 디스크에 존재하는 슬랙 스페이스의 양을 계산할 수 있음

Secondary Storage - SSD

- SSD(Solid State Drive)
- 하드 디스크 드라이브(HDD)의 현대적인 버전

- 플래터(platter)와 같은 기계식 부품이 없으며, NAND 플래시 셀이나 마이크로칩을 통해 데이터를 저장함
- NAND는 RAM에 사용되는 트랜지스터와 유사한 트랜지스터 집합으로 구성되어 있지만,
  지속적인 새로고침이 필요 없기 때문에 비휘발성 메모리 형태로 데이터를 보존할 수 있음
- 기존 HDD와 비교했을 때, 기계식 부품이 없으므로 소비 전력이 더 적고 속도가 더 빠름 (대신 더 비쌈)

	HDD	SSD
저장 방식	자기(magnetic) 방식 플래터(platter) 표면에 데이터를 기록	반도체 방식 NAND 플래시 메모리(마이크로칩)로 데이터 저장
구조	기계적 부품(플래터, 헤드 등) 포함 → 물리적 회전과 탐색 필요	기계적 부품 없음 → 전자 회로만으로 작동
속도	플래터 회전과 헤드 이동이 필요하여 상대적으로 느림	기계적 움직임이 없어 빠른 읽기·쓰기가 가능
가격/용량	대용량 대비 단가가 저렴함	동일 용량 기준 단가가 더 비쌈

HPA and DCO

[HPA(Host Protected Area)]

- 디스크 용량 일부를 의도적으로 숨기는 영역
- BIOS나 OS가 인식하지 못하도록 디스크의 총 용량 정보를 조정하여
  특정 구역을 사용 가능한 파티션 밖에 두는 형태

[DCO(Device Configuration Overlay)]

- 일부 제조사의 HDD에서 HPA(Host Protected Area) 뒤에 위치한 추가 예약 영역으로, 모든 HDD에 있는 것은 아님

- HPA와 DCO는 같은 디스크에서 공존 가능하나, 먼저 DCO가 생성되어야 함.
- 전체 디스크를 포맷해도 지워지지 않으므로 범죄자가 데이터를 은닉하기에 좋음

- 따라서, 디지털 포렌식 관점에서 숨겨진 증거가 있는지 HPA/DCO를 조사해야 함

Considerations for data recovery

구분	HDD	SSD	결과/비고
데이터 삭제 방식	파일의 포인터(인덱스)만 삭제하므로, 실제 데이터는 즉시 지워지지 않음	TRIM 명령이 즉시 실행되어 삭제된 파일의 데이터 영역을 바로 빈 공간으로 처리	HDD는 잔존 데이터가 남아 복구 가능성이 높음 SSD는 즉시 정리로 복구가 어렵거나 불가능
덮어쓰기 시점	새로운 데이터를 쓸 필요가 있을 때, 이전에 남아있던 데이터를 덮어씀	TRIM이 실행됨과 동시에 할당 해제, 이후 Garbage Collection 과정에서 실제 데이터 영역 정리	HDD는 덮어쓰기 전까지 복구 가능성 높음 SSD는 TRIM 후엔 복구 난이도 급상승
복구 난이도	실제 물리 데이터가 남아있어 상대적으로 복구 용이	TRIM으로 데이터가 즉시 지워져 복구 거의 불가능	포렌식 관점에서 SSD 복구가 훨씬 어려움
(운영체제) 특징	주로 '삭제' = 포인터 해제 파일시스템에 따라 동작 다름	운영체제마다 TRIM 정책이 달라, 즉시 실행 또는 일정 주기로 일괄 실행 가능	최신 OS 대부분 TRIM 지원, 수사 시 주의 필요

SSD는 TRIM 명령으로 삭제한 파일의 실제 데이터가 곧바로 사라져 복구가 어렵거나 불가능함

HDD는 포인터만 삭제하므로 덮어쓰기 전까지 데이터가 남아 있을 확률이 높아 비교적 복구가 쉬운 편

File system - NTFS

- Windows 운영체제는 하드 드라이브에 설치할 때, FAT 또는 NTFS을 사용
- NTFS(New Technology File System): 마이크로소프트가 개발한 고급 기능과 보안성을 갖춘 파일 시스템

- 로그(저널링) 기능을 갖추어, 갑작스러운 시스템 종료나 오류 발생 시 데이터 손상을 최소화함
- 마스터 파일 테이블($MFT) 등 여러 메타데이터 파일을 통해 볼륨에 저장된 모든 파일·폴더 정보를 관리
- Alternate Data Stream(ADS) 라는 기능으로 하나의 파일에 여러 데이터 스트림을 담을 수 있음

  디지털 포렌식 관점에서 데이터 은닉 위험 요소가 될 수 있음

- ADS 생성, 열기, 탐지, 제거: https://www.minitool.com/partition-disk/alternate-data-streams.html
- ADS를 이용해 숨겨진 파일 식별: https://www.minitool.com/partition-disk/alternate-data-streams.html
- 리눅스에서 ADS 추출하기: https://tmairi.github.io/posts/extracting-alternate-data-streams-with-linux/

File system - FAT

- FAT(File Allocation Table): 가장 오래된 파일 시스템 중 하나

  FAT12, FAT16, FAT32, FATX 버전이 있음

- NTFS보다 이식성이 뛰어나 여러 플랫폼에서 읽고 쓸 수 있음

  그러나 대용량 파일 지원이나 파일 암호화 같은 고급 기능은 부족함

	NTFS	FAT
개발/역사	마이크로소프트가 NT 계열(Windows NT, 2000, XP 등)용으로 개발	가장 오래된 파일 시스템 중 하나로, FAT12/16/32/X 등 여러 버전이 존재
지원 플랫폼	주로 Windows 운영체제에서 사용 (Mac, Linux에서는 별도 드라이버 필요)	Windows를 비롯한 다양한 OS, 디지털 카메라, 스마트폰 등 여러 기기에서 폭넓게 지원
용량 지원	대용량 볼륨 및 큰 파일(4GB 이상) 지원	FAT32의 경우 4GB 초과 파일 지원 불가
고급 기능	Alternate Data Stream(ADS), 압축 등 지원	단순한 구조로 호환성은 좋지만, 고급 기능(ADS·압축 등)은 제공하지 않음

Environment for computing

[컴퓨팅 환경별 디지털 증거 수집 특징]

- 개인용 컴퓨팅 환경
  - 특징: 모든 프로그램, 데이터가 로컬 기기에만 설치·저장(노트북, 데스크톱, 태블릿 등)
  - 장점: 증거 위치가 해당 기기에 국한 → 수사 시 상대적으로 단순함
- 클라이언트-서버 컴퓨팅 환경
  - 구성: 클라이언트(PC, 노트북, 태블릿) + 서버
  - 동작: 클라이언트가 요청 → 서버가 응답(예: 이메일 서버)
  - 포렌식 유의점: 서버 측 로그·데이터 확보 필요
- 분산 컴퓨팅 환경
  - 구성: 애플리케이션 기능을 여러 컴퓨터에 분산해서 실행
  - 데이터 저장: 여러 지역·관할 구역에 분산(원격 서버 연결)
  - 난이도: 증거 수집이 복잡(데이터·로그가 광범위하게 분산), 조사 범위 방대

디지털 증거 수집 방법은 컴퓨팅 환경 구조(개인용, 클라이언트-서버, 분산)에 따라 크게 달라지므로, 각 환경의 특성을 파악하고 적절한 수사 전략을 세워야 함

Cloud computing

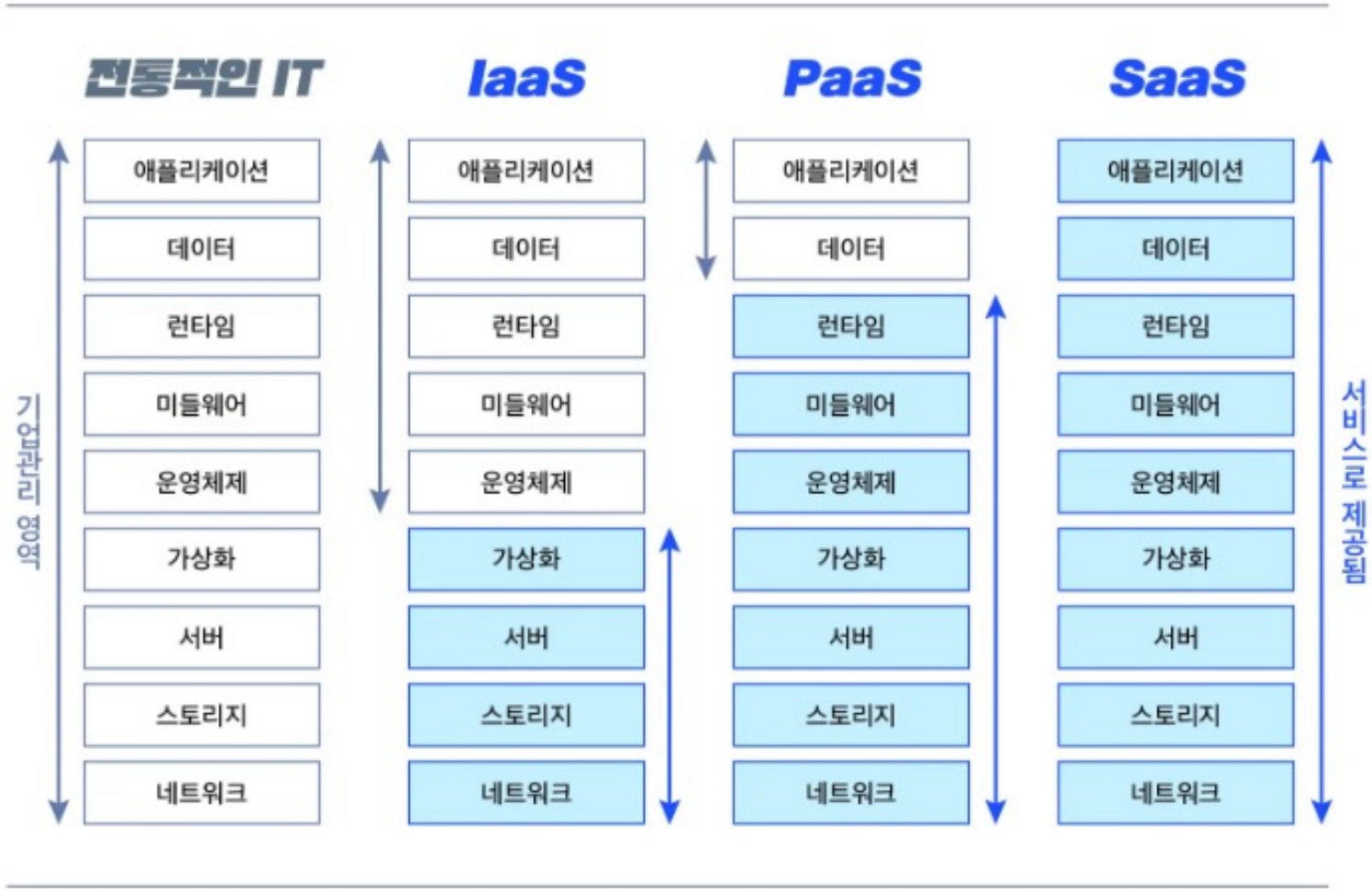
- 클라우드 컴퓨팅(Cloud computing)
- 인터넷 발달과 온라인 통신 증가에 따라, 서비스 제공자가 원격(클라우드)을 통해 다양한 컴퓨팅 자원을 사용자에게 제공하는 현대적 기술 모델

- 외장 HDD 구매 대신, 일정 비용을 내고 클라우드에 데이터 저장 → 제공업체가 데이터 백업/보호 관리
- 각 사용자마다 소프트웨어 라이선스를 따로 사지 않고, 필요 애플리케이션(예: MS Office)을 클라우드 서비스 형태로 이용 가능
- 필요한 만큼만 자원을 쓰고, 사용량에 따라 비용 지불
- 데이터 백업, 보안, 유지보수 등을 클라우드 제공업체가 담당함

SaaS / PaaS / IaaS

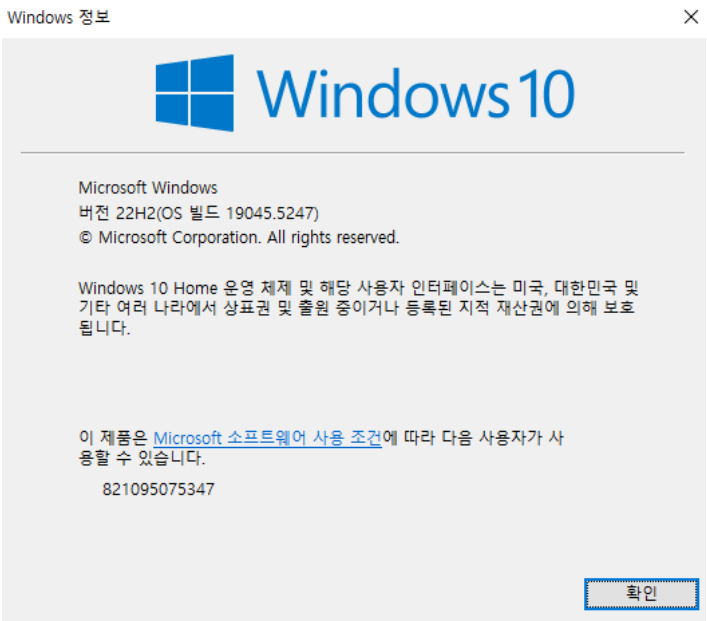
	SaaS (Software as a Service)	PaaS (Platform as a Service)	IaaS (Infrastructure as a Service)
주요 개념	완성된 소프트웨어(애플리케이션)를 클라우드에서 바로 사용	애플리케이션 개발에 필요한 플랫폼 (개발 환경, 런타임, 미들웨어 등)을 제공	네트워크, 서버, 스토리지 등 기본 인프라를 가상화하여 원격으로 임대해 주는 서비스
사용자 역할	단순히 서비스를 이용(설치·업데이트 최소화)	제공된 개발 환경에서 소프트웨어를 개발·배포	운영체제, 애플리케이션 설치 및 시스템 구성을 직접 수행
관리 범위	서비스 제공업체가 애플리케이션 전체와 기반 인프라 관리	서비스 제공업체가 플랫폼(서버, OS, 런타임) 관리 사용자는 개발된 앱 관리	서비스 제공업체가 물리적 하드웨어(서버, 네트워크 등) 관리 사용자는 가상 머신, OS, 미들웨어 등 구성
장점	설치·유지보수 부담 감소 즉시 사용 가능	개발 환경 설정 시간 단축 인프라 관리 부담 감소 확장성 용이	물리 서버 구매 없이 인프라 확장 사용량 기반 요금(비용 최적화)
단점	사용자 맞춤 기능 제한 커스터마이징 범위 제한	특정 플랫폼 종속성	사용자가 OS, 미들웨어, 앱 유지보수 필요
예시 서비스	Google Workspace, Microsoft Office 365 등	Microsoft Windows Azure, AWS Elastic Beanstalk, Google App Engine	AWS, Google Cloud, IBM Cloud 등

SaaS / PaaS / IaaS



Windows versions

- 디지털 포렌식 수사관은 증거 수집 및 분석 단계에서
  Windows 운영체제 버전 간의 차이점을 파악하기 위해
  현재 Windows OS 정보를 어떻게 수집하는지 알아야 함



- Windows 8 이상: Windows 키 + R 키
  검색 창에 winver 입력 후 Enter

- Windows 7의 경우에는 제어판(Control Panel) > 시스템(System)으로 이동한 후,
  Windows 에디션 항목에서 현재 버전 정보 확인

Getting an IP address

- IP (Internet Protocol) address
  - 컴퓨터/네트워크 기기의 고유 식별자, 하나의 IP 네트워크에서 중복 불가
  - 일반적으로 TCP(전송 제어 프로토콜)와 함께 사용되어 목적지·소스 간 가상 연결을 설정

- IPv4와 IPv6
  - IPv4(32비트): 약 43억 개 주소, 현재 대부분의 인터넷 서비스에서 사용
  - IPv6(128비트): IPv4 주소 부족 문제 해결을 위해 개발, 훨씬 더 많은 주소 지원

- 공인 IP 주소(Public IP)
  - ISP가 할당, 직접 인터넷에 연결할 수 있는 유일한 주소
  - 고정 IP(Static): 한 번 할당되면 잘 바뀌지 않음(전화번호와 유사)
  - 동적 IP(Dynamic): 사용자가 인터넷에 접속할 때마다 새 주소 할당 -> DHCP 프로토콜을 통해 자동으로 배정

- 사설 IP 주소(Private IP)
  - 라우터 뒤(내부 네트워크)에서 인터넷에 직접 노출되지 않는 주소
  - 가정·학교·회사 등 폐쇄형 네트워크에서 사용
  - 보통 라우터의 DHCP를 통해 자동 할당
  - 여러 기기에서 중복 사용 가능(서로 다른 내부망은 중복 가능하나, 공인 IP와는 분리됨)

Conclusion

- 디지털 포렌식 수사관이라면 잘 이해하고 있어야 할 컴퓨터 관련 중요 기술 개념들을 소개함

- 컴퓨터가 데이터를 어떻게 저장하여 디지털 방식으로 표현하는가?
- 운영체제 파일 구조와 그 유형은 무엇인가?
- 해시 알고리즘을 이용해 디지털 데이터의 진위(무결성)를 어떻게 확인할 수 있었는가?

위 질문에 대한 대답을 얻는 시간이었기를 바랍니다~

END OF PRESENTATION

SLIDE: 34

THANK YOU FOR YOUR ATTENTION