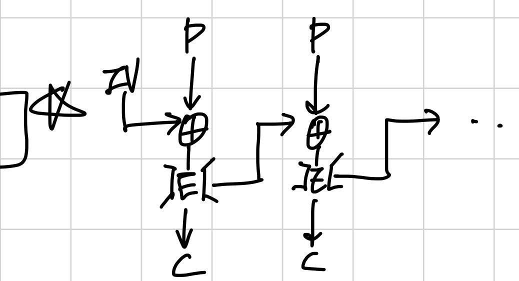
해시함수

- 해시함수의 보안 요구사항
  - ① 역상 저항성 — "원본" (프리이미지 저항성)
  - ② 약한 충돌 저항성 — "주어진" (2차 역상 저항성)
  - ③ 강한 충돌 저항성 — "임의"
- 가장 기본 구조 — 조건: "언제나" "일정크기" 출력.
  - 「반복」 ㄴ 고정길이 입력 - 고정길이 출력.
  - ↓ Merkle-Damgard
    - ㄴ 핵심: compression function 이 "반복해시함수"
- 키의 유무
  - 키가 없는 해시함수
    - 용도 — MDC (변경감지코드) 무결성 check 등..
    - 종류
      - ① 전용
        - ① MD5 (2→4→5) 512 bit → 128 bit ↔ Birthday Attack
        - ② SHA-1, -2 // big endian (160, 224, 256, 384, 512) — input 512 bit / input 1024 bit
        - ③ RIPEMD-160 (안전함) (512→160)
        - ④ Tiger, HAVAL
      - ② 블록암호 기반
      - ③ 모듈 연산 기반 // 내장된 모듈연산
  - 키가 있는 해시함수
    - 용도 — "MAC" 메시지 인증 (송신처 보장)
      - ㄴ 근거: 키의 비밀성 + 함수의 보안성.
    - 종류 → 블록암호 기반 "CBC"

(SHA-1, -2 모두 用)
SHA-512 (1024→512) → KECCAK (SHA3)

Original message + Padding + Original length (128 bits) = n * 1024 bit



MAC

- nested MAC (축소 MAC): H(K+H(K+msg))
- HMAC
  - (K+pad) → ipad 0x36 ⊕ → + msg → Hash
  - opad 0x5C ⊕ → + Hash → Hash → HMAC
- ① Replay ↔
  - ① seq #
  - ② timestamp
  - ③ nonce
  - ④ challenge—Response
- 부인방지 주의 / 제 3자에 대한 공격 주의 → 전자서명 등장.

CBC-MAC —보완→ CMAC
- + CTR → CCM
- + AUTH → GCM.

DoS

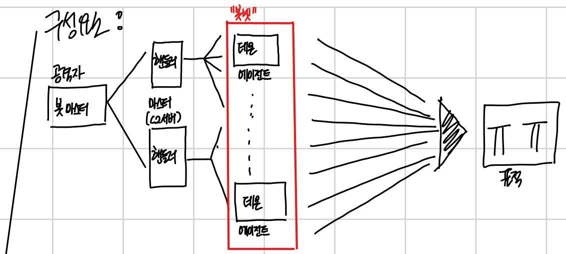
「단일」 컴퓨터로 공격!

- 취약점 익스플로잇 (Poison 패킷)
  - PoD
    - 'Ping' ∴ ICMP Echo Request.
    - 매우 큰 ICMP를 Fragmentation ⟷ 일반 ICMP는 Fragmentation 할 이유 X.
      - ✻ ICMP Echo Req
        - UNIX/LINUX : 56 byte
        - Windows : 32 byte
  - LAND
    - "IP Spoofing"
    - ip.dst : ip.port == ip.src : ip.port 전부 공격대상 것으로.
  - Teardrop
    - 원리: IP 헤더 – Fragmentation offset 악용.
    - 종류
      - Open tear attack : Fragmentation 플래그 설정해 놓고 실제로는 안함.
      - 변종
        - Bonk : Fragmentation Offset == 1 (all)
        - Boink : 중간에 갑자기 offset을 이상하게 보냄.
- Flooding
  - TCP SYN Flooding
    - 원리: TCP Half-open 악용. SYN → SYN+ACK → ⁝ 서버: 답答 뭐;; (머리아짐)
      - → By 애초에 src addr spoofing 해서 ACK가 엉뚱한 데로 감.
    - 대책
      - 연결 대기 수
        - 직접 : TCP 연결 대기열↑
        - 간접 : TCP 연결 대기열 엔트리 삭제, 동일 IP의 SYN 한계치 설정
      - 공격 특징 역이용
        - first SYN drop
        - '라우터'가 위조 IP주소 패킷 필터링.
      - 인증 – TCP SYN_Cookie 用. – SYN → S+A+"SYN_Cookie" → 세션 close
  - SMURF
    - 원리: 「증폭」
      - 공격자 → 증폭 네트워크 ⇉ 공격, // ICMP Echo req & reply + IP Spoofing + Broadcast by Directed Broadcast addr (NetID+255)
    - 대책
      - '라우터'가 인바운드 Directed-Broadcast 패킷 필터링
      - '호스트'가 브로드캐스트 ICMP 패킷 Drop.
      - '호스트'가 대량의 ICMP Echo Reply 가 오면 Drop.
  - Fraggle
    - 원리: 7/UDP가 echo 서비스임을 악용.
      - 7/UDP가 닫혀 있더라도 UDP 특성상 ICMP Unreachable 발생.

DDoS

'물리적으로 다수' 컴퓨터로 공격!

- 구성요소 :



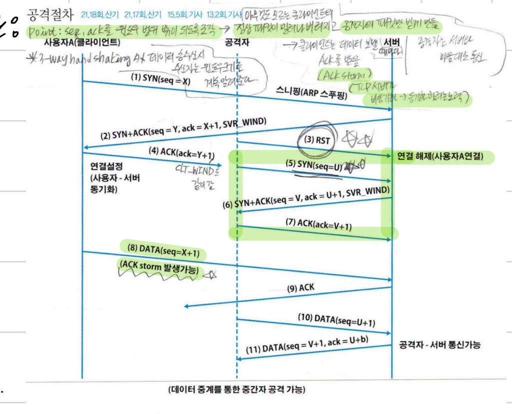
- 전통
  - Trinoo : UDP用 ∴ Fraggle
  - TFN : TCP, ICMP用 ∴ SMURF, PoD, TCP SYN Flooding
  - Stacheldraht : 마스터–에이전트 통신 암호화 (참고 / 업그레이드)
  - TFN2K : UDP도 用, 마스터–에이전트 통신 암호화 & 랜덤포트., 백도어 설치可
- 최신
  - ① 대역폭 공격 (높은 bps / UDP, ICMP, TCP)
    - Flooding
      - UDP
      - ICMP (!= SMURF ∵ 증폭서버 X)
    - Reflected → DRDoS
      - TCP
      - ICMP
      - ☆ UDP → DNS, Memcached, ..
  - ② 자원소진 공격 (높은 bps, connection 수 / TCP)
    - TCP SYN Flooding : bps << pps = 이상하게 커넥션이 많음
    - TCP Ack Flooding : 무수한 ACK에 RST or ICMP Unreachable 응답하느라...
    - (53) DNS Query Flooding : DNS 서버가 타깃
  - ③ 웹/DB 부하 공격. (높은 pps, connection 수 / HTTP, HTTPS)
    - GET Flooding : HTTP GET
      - CC Attack : GET Flooding with Cache-Control: no-store, must-revalidate (HTTP 304 무력화)
    - Slowloris : HTTP Header (CR, LF)
    - RUDY : HTTP POST
    - Slow Read : TCP window_size : window_size 매우 작게, 고의 지연으로 통신 → 이게 쌓이면 TCP Connection 자원 고갈.
    - 동적 HTTP Request Flooding : 요청 페이지 변경해가면서 요청.
  - ④ 기타
    - HashDoS
    - HulkDoS
    - SIP Flood.

Port Scanning

- Open 스캔
  - TCP 스캔
    - TCP Full Open
      - 과정 : SYN → SYN/Ack → Ack
      - 가능결과 :
        - 포트 open : SYN → SYN+Ack
        - 포트 closed : SYN → RST+Ack
    - TCP Half Open (SYN 스캔)
      - 과정 : SYN → SYN+Ack → RST.
      - 가능결과
        - 포트 open : SYN → SYN+Ack → RST
        - 포트 closed : SYN → RST+Ack
  - UDP 스캔
    - 가능결과
      - 포트 open : No Reply
      - 포트 closed : ICMP Unreachable
    - 신뢰도 : 낮음 ∵ 라우터. 방화벽에 의해 손실可.
- Stealth 스캔
  - ☆ TCP Ack 스캔 : 「방화벽 룰셋」 테스트용
    - 목적 정보
      - 방화벽이 Stateful 인가? (상태 기반)
      - 대상 포트가 방화벽에 의해 필터링되는 中인가?
    - 가능결과
      - filtered : ICMP Unreachable or No Reply
      - not filtered : RST
  - TCP FIN, NULL, X-MAS 스캔 – 가능결과
    - 포트 open : No Reply
    - 포트 closed : RST
  - TCP Fragment 스캔

✻ Nmap 명령어 :
- -sU : udp scan
- -sP : Ping scan
- -sD : Decoy scan
- -b : FTP bounce scan
- -p : 포트 옵션.
  - -p 1–1023 (범위)
  - -pT:2,5,10, U:2,30,10 TCP와 UDP 포트 구분可.

세션 하이재킹
- TCP 연결 하이재킹 "active" ∴ 명령실행可.
  - 순서번호 추측기반 : TCP의 seq#를 추측해 사용자-서버 간 TCP 세션 가로챔.
    - → 공격자 → 서버(o) // 공격자 ← 서버(x) ∴ 일방향 통신으로만 공격 작업可. ⟷ 시작 순서번호(ISN) Randomize
  - 스니핑 기반 :



* Ack Storm 가능성.

- 웹 세션 하이재킹 : 세션id 가로챔.

스니핑
- L1 : 허브, promiscuous
- L2 : 스위치, MAC Address Table Overflow → Fail Open ⊕ 스위치의 SPAN/Port Mirroring 기능 有.
  - MAC 変, ARP Reply 계속 전송.

스푸핑
- L2 : ARP — ARP Reply
  - Spoofing : 특정 호스트인 척! (점대점)
  - Redirecting : 특정 라우터인 척! (점대다)
  - * ARP는 L3지만 공격은 로컬에서 ∴ L2공격.
  - ⟷ ARP 캐시 테이블의 정적구성 by arp -s ip mac (리부트 시 static 풀림)
- L3 :
  - ICMP Redirecting : 타깃 호스트에게 자기가 더 효율적인 라우터인 척! — ICMP Redirect
    - → 이후 진짜 라우터에게 Relay
  - IP Spoofing : C-B 통신에서, B에는 DoS 걸어두고 자기가 B인 척 C와 통신
    - MIM ⟷ IPSec (인증)
- \+ e-mail spoofing
- L7 : DNS Spoofing : DNS 패킷은 UDP ∴ 세션无 악용. 실 DNS서버보다 빨리 DNS Response 보냄.
  - "시간차 공격"
  - * DNS lookup 수행 순서
    - ① 내부 캐시 ② hosts 파일 ③ DNS Query → 서버에 질의

요약:

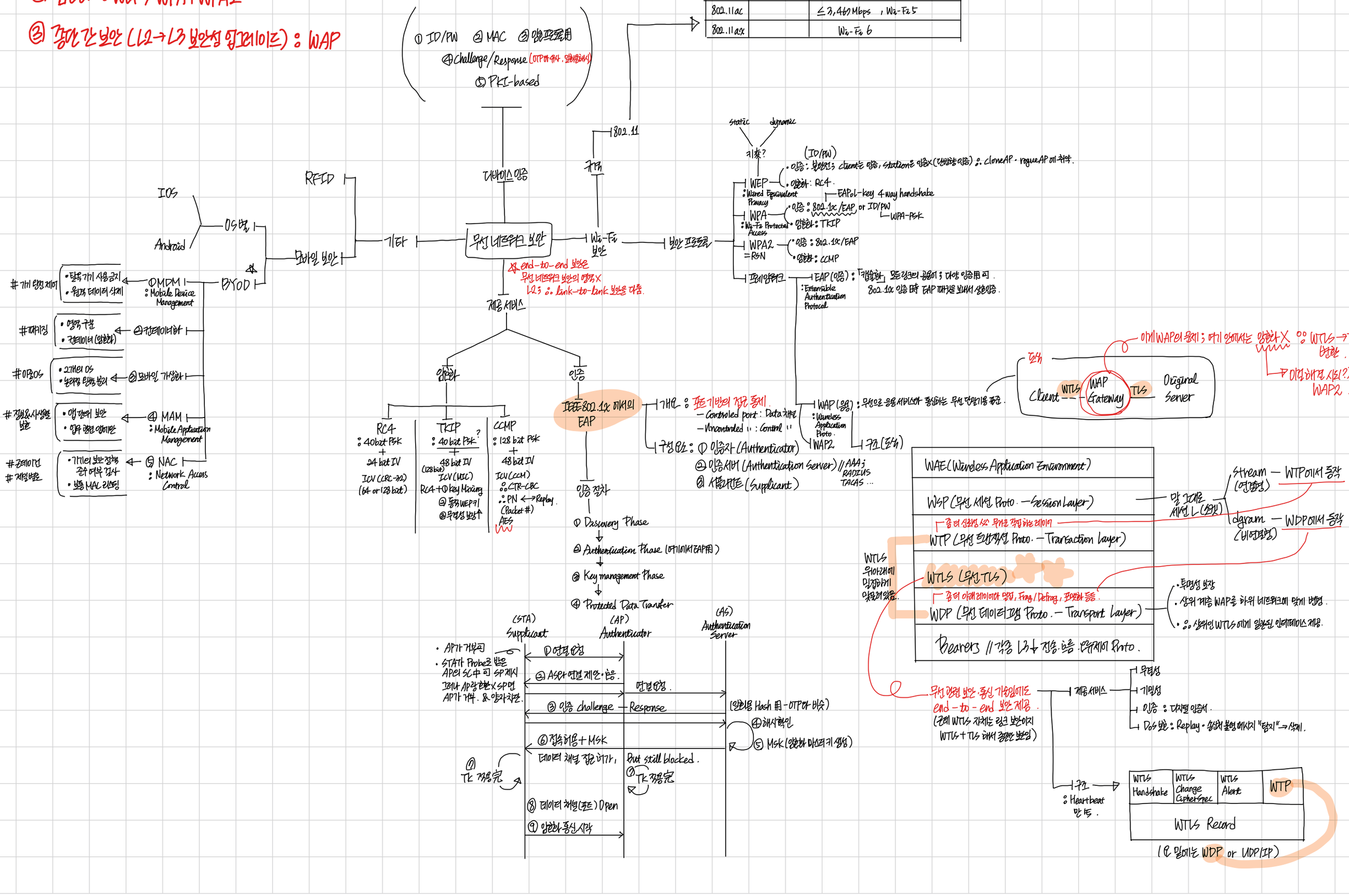
무선 환경에서의 보안을 위해

① 인증 : 802.1x-EAP

② 암호화 : WEP, WPA, WPA2

③ 종단 간 보안 (L2→L3 보안성 업데이트) : WAP

802.11b	2.4GHz/11Mbps	WEP 지원
802.11a	5GHz/54Mbps	동심개념 · 환형개념
802.11g	2.4GHz/54Mbps	
802.11i	2.4GHz/11Mbps	802.11b+보안성 (여기 WPA&WPA2임)
802.11n	5GHz, 2.4GHz	≤600Mbps, MIMO(다중IO · 여러안테나)
802.11ac		≤3,467Mbps , Wi-Fi 5
802.11ax		Wi-Fi 6



- 악의X
  - 디스크
    - sector gap : 파일 트랙의 쓰지 X 공간
    - slack area : 파일 크기 != 클러스터 크기
  - 인터넷 임시파일
    - ① 임시 인터넷 캐시 : [SystemRoot]₩Downloaded ProgramFiles ②
    - [UserProfile]₩Local Settings₩
      - Temporary Internet Files : 임시 인터넷 파일 ③
      - History : 방문했던 웹페이지 ⑤
      - COOKIES : 임시 쿠키 파일 ④
- 악의 데이터 은폐
  - 데이터 암호화
  - 스테가노그래피
- 데이터 파괴
  - 드라이브 와이핑 (내용 지우기)
  - 디스크 디가우징 (디스크 자기장 지우기)
- Anti-Forensic

침해사고대응

- CERT
  - 4개 역할
    - ① 침해사고 예방/대응 기술 연구·전파
    - ② 침해사고 예방
    - ③ 침해사고 대응
    - ④ 외부 기관과 대응협력 활동
  - 사고대응 7개 절차 : 사고 전 준비 → 사고 탐지 → 초기 대응 → 대응 전략 체계화 → 사고 조사 → 보서 작성 → 복구·해결
- 디지털 포렌식
  - 포렌식의 5개 기본 원칙
    - ① 정당성의 원칙
    - ② 재현의 원칙
    - ③ 신속성의 원칙
    - ④ 연계 보관성의 원칙 (chain of custody)
    - ⑤ 무결성의 원칙 - by 해시값.
  - 수행 5개 절차

사전 준비 → 증거 수집 → 보관 및 이송 → 조사 및 분석 → 보서 작성

- 사전 준비
  - *디스크 이미징
- 증거 수집
  - *Evidence Sage
- 보관 및 이송
  - *최량증거원칙 (original)
- 조사 및 분석
  - *조사기법
    - 디스크 브라우징
    - 데이터 복구
    - 파일 복구
- 보서 작성