시스템 정보 수집 결과 요약

1. 시스템 정보 수집 시작/종료 일시

- 시작: **2025-09-18 14:58:02**
- 종료: **2025-09-18 14:58:49**

2. OS 및 네트워크, 윈도우 기본 정보

system_info

- **호스트명**: DESKTOP-SA342QM
- **OS**: Microsoft Windows 11 Pro (빌드 22631)
- **제조사/모델**: LG Electronics 15U50R-G.AP5VLF
- **CPU**: Intel64 Family 6 Model 186 @ ~1300MHz (1개)
- **메모리**: 총 16,122MB (사용 가능 5,776MB)
- **도메인**: WORKGROUP
- **네트워크 카드**:
  - Wi-Fi 2: IP 192.168.0.18 / DHCP 192.168.0.1
  - VMware VMnet0: IP 169.254.197.203 (가상 어댑터)

3. 사용자 정보

users

- 계정 목록: Administrator, DefaultAccount, Guest, User, WDAGUtilityAccount
- 현재 세션: **User (ID 23, console, 활성)**- 로그인 시각 2025-09-18 08:59

4. 공유 정보

shares

- **C$**→ C:₩ (기본 공유)
- **ADMIN$**→ C:₩Windows (원격 관리)
- **IPC$**→ 원격 IPC

5. 시스템 기본 보안설정

firewall

- 방화벽 상태: **도메인 / 개인 / 공용 프로필 모두 활성화됨**

6. 실행 중인 서비스 목록

services

- Application Information (Appinfo)
- Application Management (AppMgmt)
- Windows Audio / AudioEndpointBuilder
- Base Filtering Engine (BFE)
- BrokerInfrastructure (백그라운드 작업)
- Bluetooth 관련 서비스

  ☞ 시스템 주요 보안·네트워크·오디오 서비스 정상 동작 중

7. 공유된 파일 실행 여부

- **직접 실행 흔적 없음**(공유는 C$/ADMIN$/IPC$ 기본 공유만 활성화)
- shares

8. 프로세스 정보

processes

- **보안 관련**: MsMpEng.exe (Windows Defender, 422MB)
- **로그 관련**: splunkd.exe (Splunk, 212MB)
- **DB/개발**: mongod.exe (MongoDB), python3.9.exe 실행 중
- **기타**: agent-manager.exe, identity.exe, Steam, Discord 등

9. 네트워크 관련 정보

network_info

dnscache

- 로컬 IP: 192.168.0.18
- 열려있는 포트:
  - TCP 8000, 8089 → Splunk
  - TCP 8191 → MongoDB
  - TCP 8065 → python3.9.exe

외부 연결:

- 4.213.25.242:443, 104.18.32.47:443 등 HTTPS 세션

DNS 캐시:

- Steam 서버: p2p-seo1.discovery.steamserver.net → 146.66.152.x
- Microsoft Edge 서비스: default.exp-tas.com → msedge.net

10. 파일 생성(C) / 수정(M) / 접근(A) 이력

recent_files

- **C:₩forensic*경로에 다수 로그 파일 생성 (2025-09-18 14:58 수집 결과)
- Windows / OneDrive 업데이트 관련 파일 다수 수정 기록
- 기타: 최근 하루 내 생성/수정된 실행 파일은 별도 포착 없음

11. 시작프로그램 목록

autoruns_registry

- **정상 범주**: OneDrive, KakaoTalk, Discord, Steam, RiotClient, Edge 자동실행
- **의심 항목**:
  - Report_Updater→ 실행 파일이 아닌 **Python 스크립트 등록** (practice_PE.py)