레지스트리란? -> 윈도우에서 컴퓨터 하드웨어, 응용프로그램, 서비스, 보안 및 사용자들에 대한 세팅 등 전반적인 설정을 담는 중앙 계층형 데이터베이스

레지스트리 루트키

1. HKEY_CLASSES_ROOT
 - 파일 확장자명과 이에 연결되는 Application 정보, COM 객체 등록 정보

2. HKEY_CURRENT_USER
 - 현재 시스템 상 로그인된 사용자 정보(C:\Users\<username>\NTUSER.DAT)
 - HKEY_USERS에 대해 우선권을 가짐

3. HKEY_LOCAL_MACHINE
 - 시스템 전체 H/W, S/W 정보, 드라이버나 환경 설정 사항

 1) HKEY_LOCAL_MACHINE\HARDWARE
 - 부팅시 감지된 H/W와 이의 드라이버 매핑 정보 (장치관리자)
 - 시스템 상 파일로 존재 X, 메모리 상 휘발성 정보로만 존재

 2) HKEY_LOCAL_MACHINE\SAM
 - 사용자 PW, 소속 그룹, 도메인 정보 등 로컬 계정 정보 및 그룹정보 저장
 - 컴퓨터가 도메인 컨트롤러일 경우, 액티브 디렉토리(AD서버)에 도메인 계정/그룹 정보 저장

 3) HKEY_LOCAL_MACHINE\SECURITY
 - 시스템 범위의 보안 정책, 사용자 권리 할당 정보

 4) HKEY_LOCAL_MACHINE\SOFTWARE
 - 시스템 범위의 S/W 목록, 환경설정 정보(Application의 이름, 경로 등)

 5) HKEY_LOCAL_MACHINE\SYSTEM
 - 시스템 부팅 시 필요한 시스템 환경 설정 정보(디바이스 드라이버, 시작 서비스 목록 등)
 - 부팅 복사본 생성 및 백업

4. HKEY_USERS
 - 시스템 상 모든 계정/그룹에 관한 정보 (서브키가 HKCU와 동일)

5. HKEY_CURRENT_CONFIG
 - 시스템 시작 시 사용되는 H/W 정보
 - 부팅 시 생성, Disk 적재 X

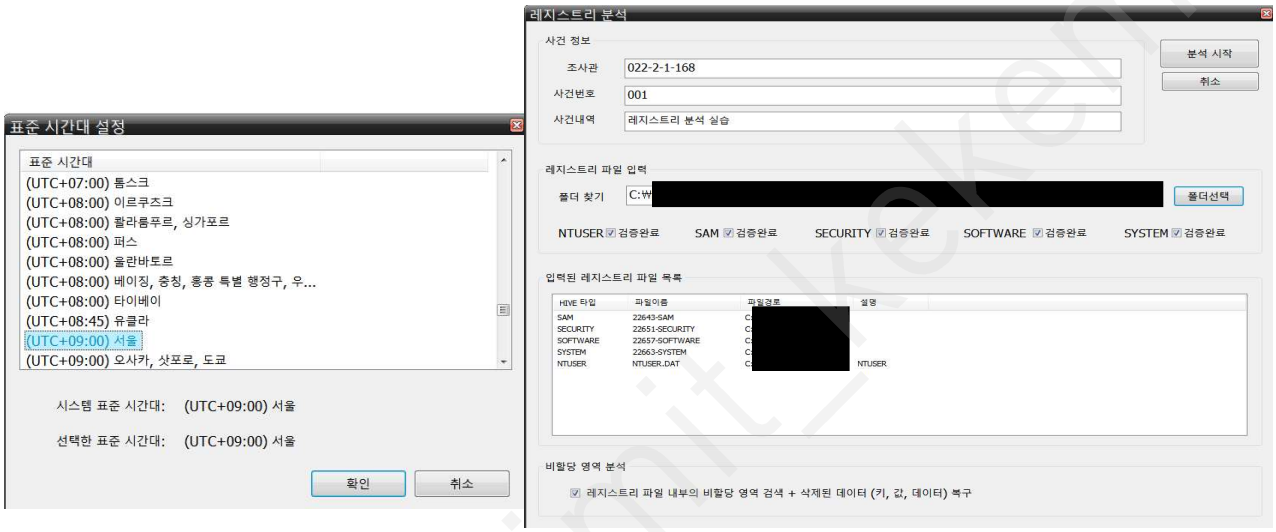
6. HKEY_PERFORMANCE_DATA
 - 런타임 성능 정보
 - 레지스트리 편집기에서 보이지 않음 (WinAPI 명령어로 열람 가능)

레지스트리 하이브 파일 분석 (REGA 1.6.0.0 이용)

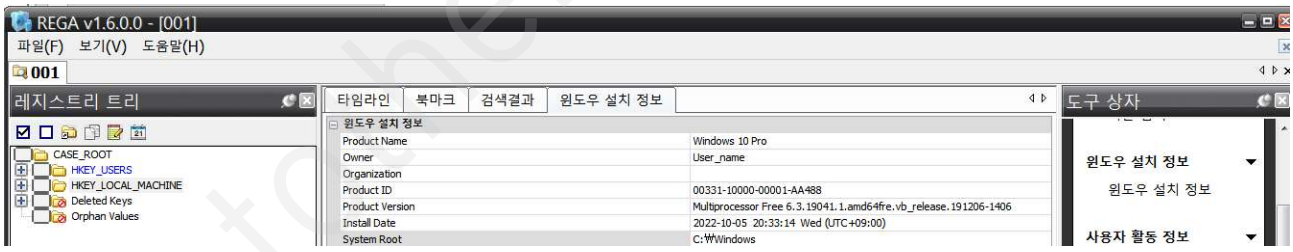
해당 시스템 내 Windows 깔려 있는 볼륨(파티션) 내 '%SystemRoot%\System32\config\' 하위 SYSTEM, SAM, SECURITY, SOFTWARE 추출,

'C:\Users\(각 사용자 계정 폴더)\' 하위의 'NTUSER.DAT' 각각 추출함.

REGA 실행 후 '(UTC+09:00) 서울' 표준시간대 설정
추출된 레지스트리 파일 입력하여 분석 시작.

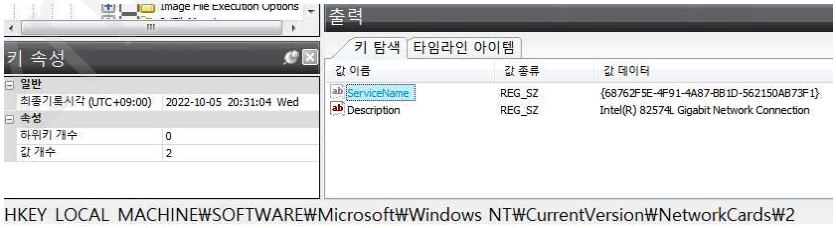


1. Windows 설치 정보 확인



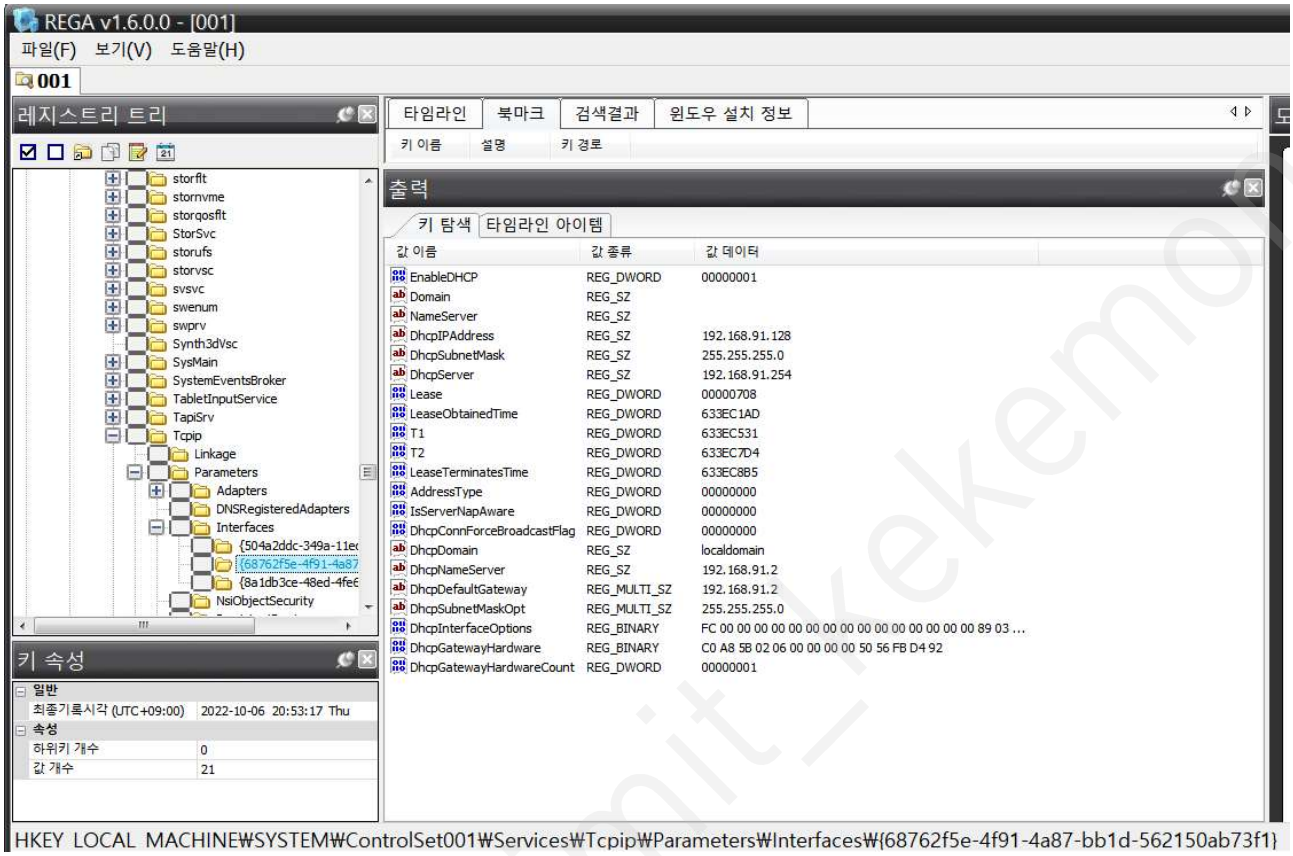
2. 네트워크 카드(NIC) 정보 확인

1) 모델명 및 GUID 확인



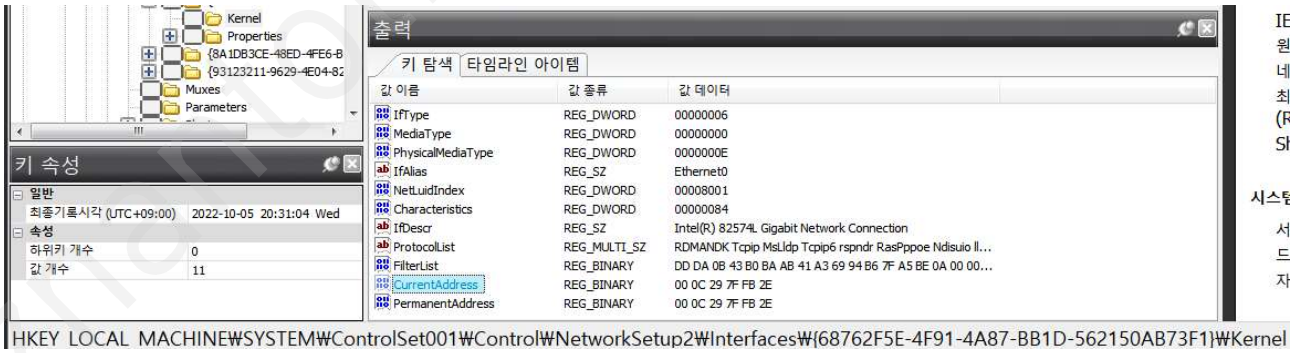
모델명 및 GUID 확인을 위해 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\' 하위 검색

2) DHCP IP Address 확인



'HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\(해당 식별자;GUID)' 하위 값(Dhcp IPAdress/SubnetMask/Server, DhcpNameServer) 검색하여 DHCP IP Address 및 부가 정보 확인.

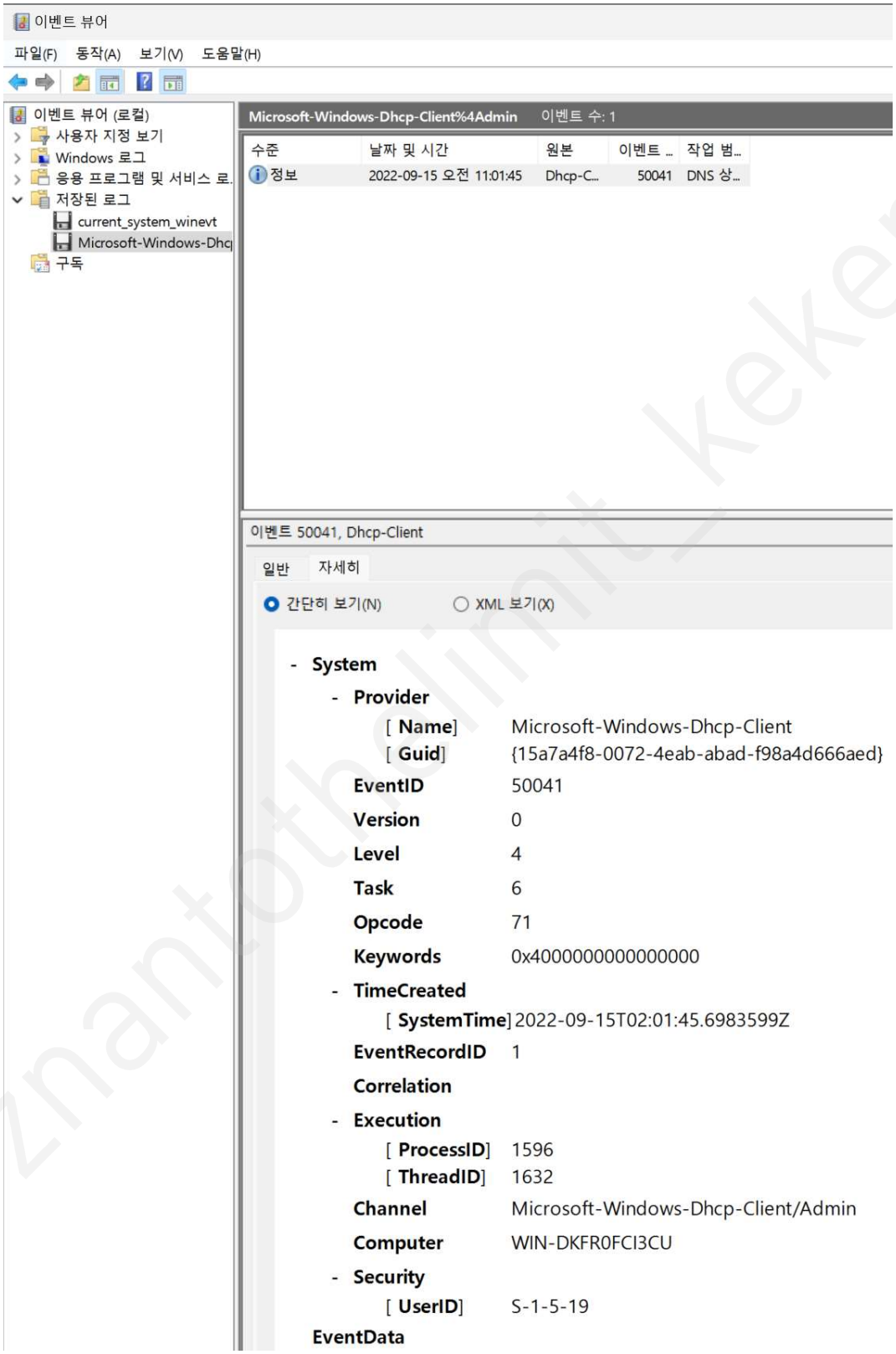
3) MAC Address 확인



'HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\NetworkSetup2\Interfaces\{GUID}\Kernel\' 키 내 MAC Address 확인

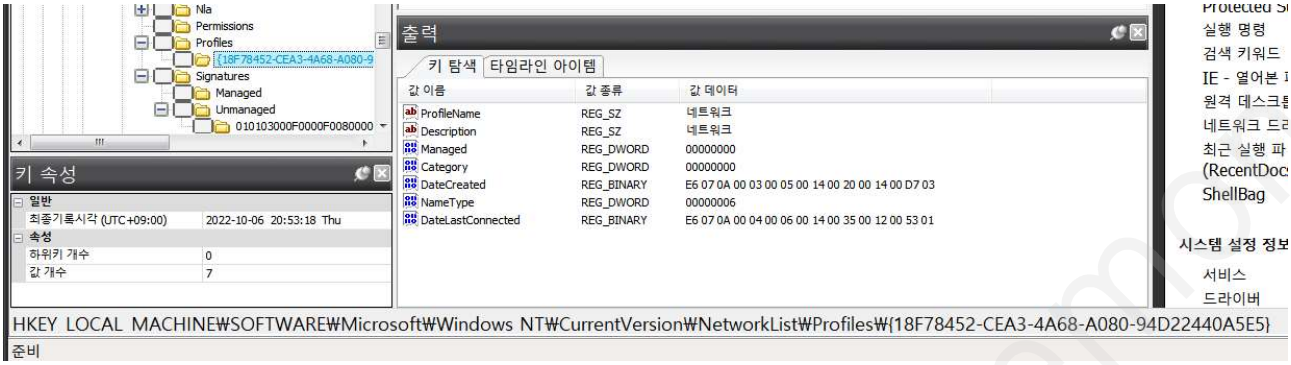
추가) 이벤트 로그 확인(무선 네트워크일 시)

'/Windows/System32/winevt/Logs/Microsoft-Windows-Dhcp-Client%4Admin.evtx' 추출하여 이벤트 뷰어에서 열기



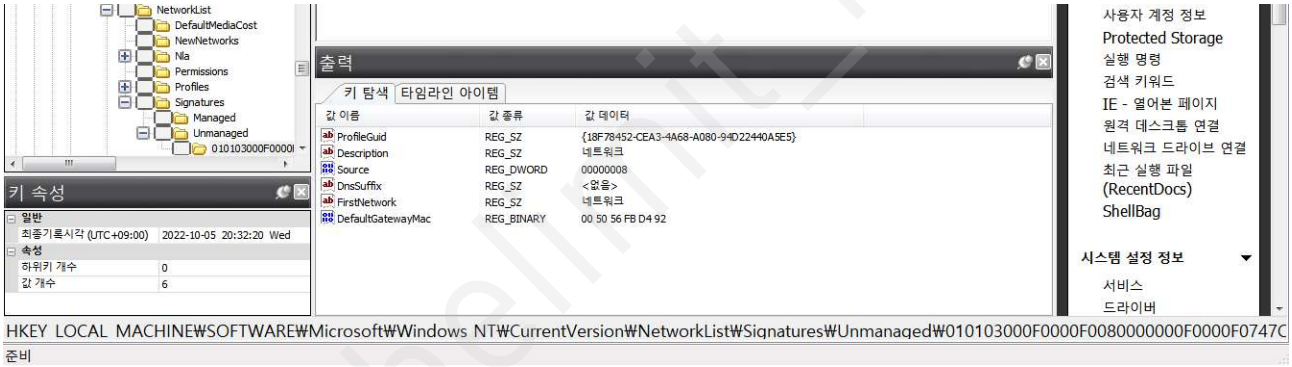
3. 유·무선 공유기 정보 확인

1) 네트워크카드(NIC) 정보 확인



‘HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\(공유기의 GUID)\’의 하위 값들로 SSID(해당 네트워크 이름), 최초/최종 접속일시 정보 확인

2) MAC Address 확인



‘HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\’하위 키(Managed 또는 Unmanaged) 선택하여 MAC Address 확인