Windows 및 MacOS에서 보안 클라이언트에 대한 KDF 로그 수집

목차

[소개](#)

[Windows 및 MacOS 플래그](#)

- [KDF 로그, Wireshark 및 DART 번들 수집](#)
  - [창](#)
  - [MacOS](#)

[관련 정보](#)

소개

이 문서에서는 Windows 및 MacOS에서 KDF 로그 및 기타 중요한 문제 해결 로그를 수집하는 방법에 대해 설명합니다.

Windows 및 MacOS 플래그

DNS 관련(OpenDNS가 포함된 경우):	0x20801ff
웹 흐름(SWG) 프록시 및 DNS 관련:	0x70C01FF
ZTA	0x400080152

KDF 로그, Wireshark 및 DART 번들 수집

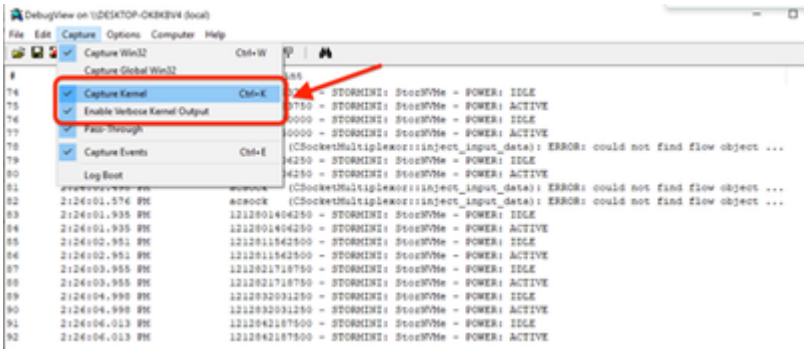
참고: 결과를 제출할 때는 항상 TAC 팀에 어떤 설정이 사용되었는지 알리고 TAC에서 요구하는 대로 변경할 수 있도록 합니다.

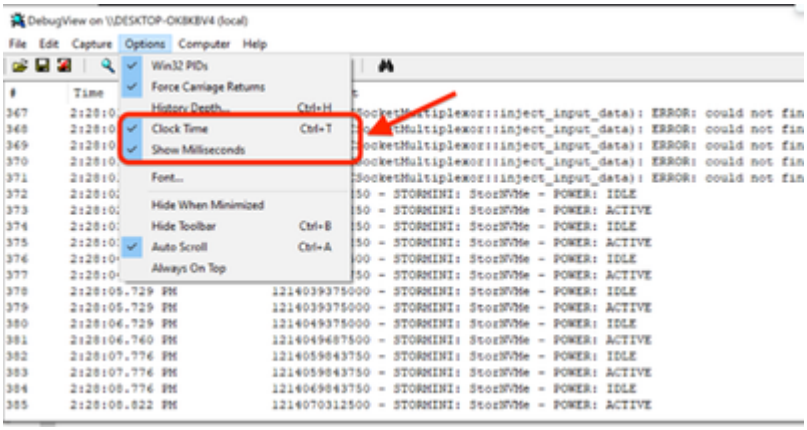
창

관리자 권한으로 CMD를 열고 다음 명령을 실행합니다.

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf [FLAG]
```

- SysInternal에서 DebugView를 다운로드하여 KDF 로그를 캡처합니다.
- 다음DebugView으로administrator실행하고 다음 메뉴 옵션을 활성화합니다.
- Capture(캡처)를 클릭합니다
    - 확인 표시 Capture Kernel
    - 확인 표시 Enable Verbose Kernel Output
- 옵션
    - 확인 표시 Clock Time
    - 확인 표시 Show Milliseconds

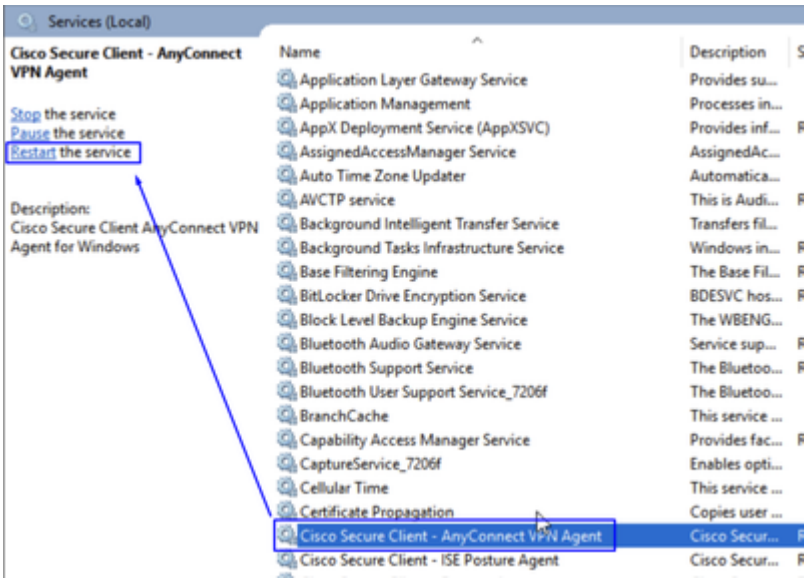




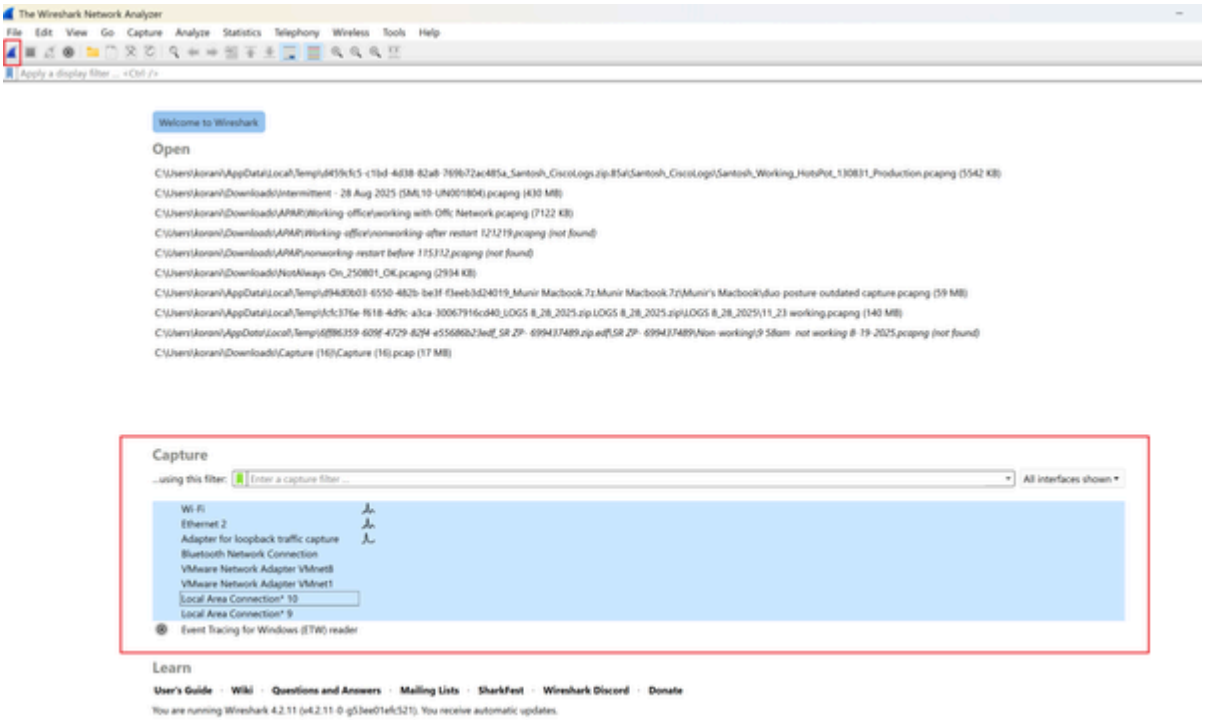
- 관리자 프롬프트를 통해 클라이언트 서비스를 다시 시작합니다.

```
net stop csc_vpnagent && net start csc_vpnagent
```

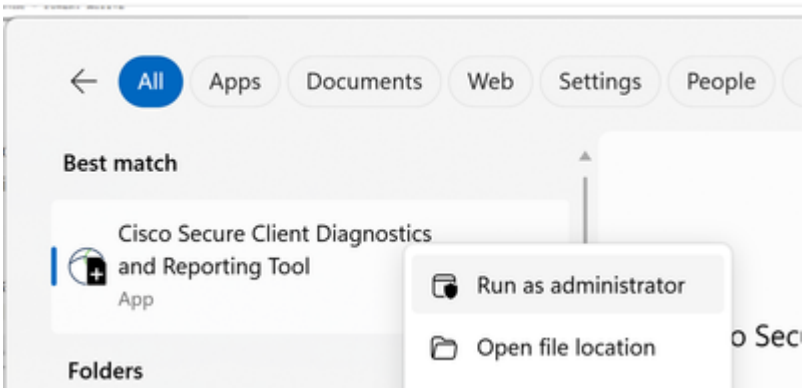
- 작동이net stop csc_vpnagent && net start csc_vpnagent되지 않으면 services.msc에서 서비스를 다시Cisco Secure Client시작합니다.



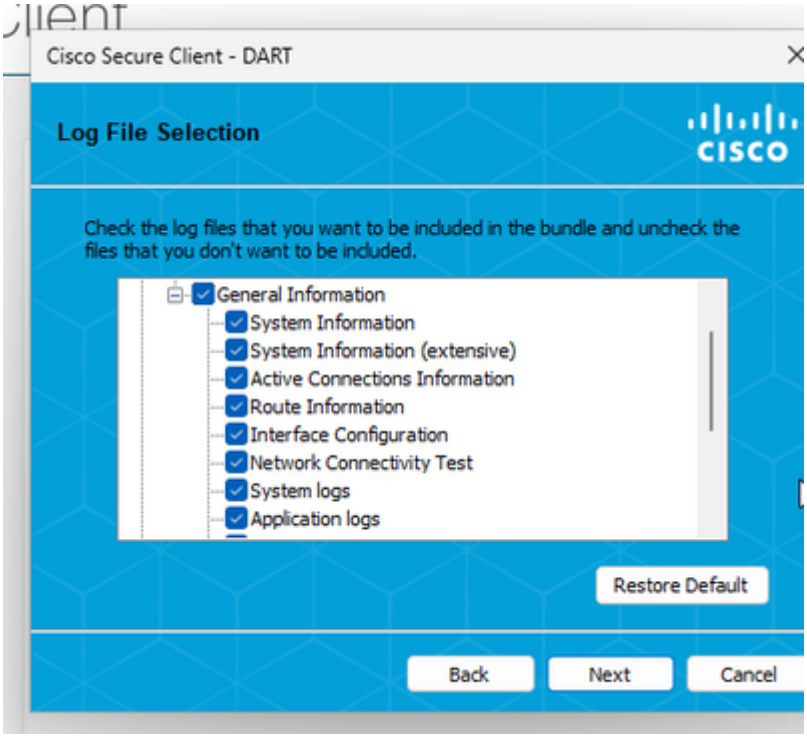
- 시작하기 Wireshark Capture
- 모든 인터페이스를 선택하고 패킷 캡처를 시작합니다



- 문제를 재현하고 저장KDF Logs및Wireshark Capture다음 캡처할 단계를 수행합니다. DART Bundle
- 관리자 권한으로Cisco Secure Client Diagnostics & Reporting Tool (DART)를 엽니다



- 클릭 Custom
  - 포함System Information Extensive및 Network Connectivity Test



참고: 모든 로그, KDF 로그, Wireshark 캡처 및 DART 번들을 TAC 케이스에 수집합니다.

- Windows에서 KDF 로깅을 중지하려면 다음 명령을 사용합니다.

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -cdf
```

MacOS

터미널을 열고 다음 명령 체인에 따라 MacOS에서 KDF 로깅을 활성화합니다.

- Stop Service

```
sudo "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app/Contents/MacOS/Cisco
```

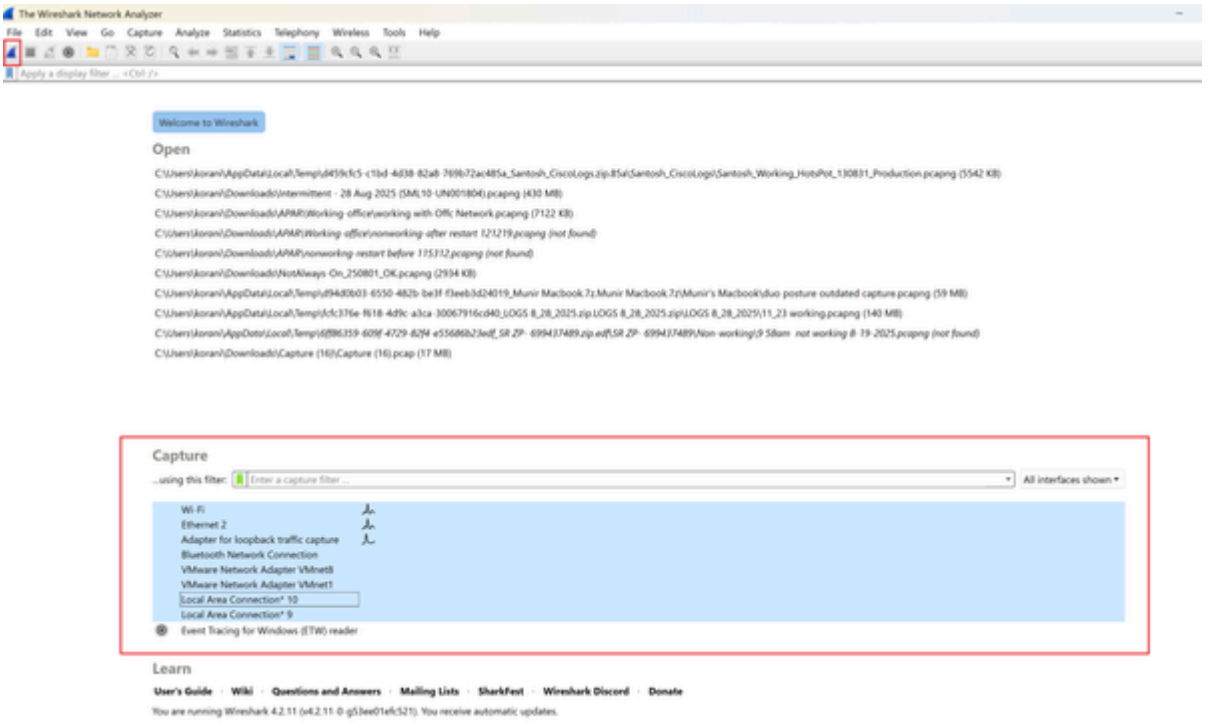
- Enable Flag

```
echo debug=[Flag Value] | sudo tee /opt/cisco/secureclient/kdf/acsock.cfg
```

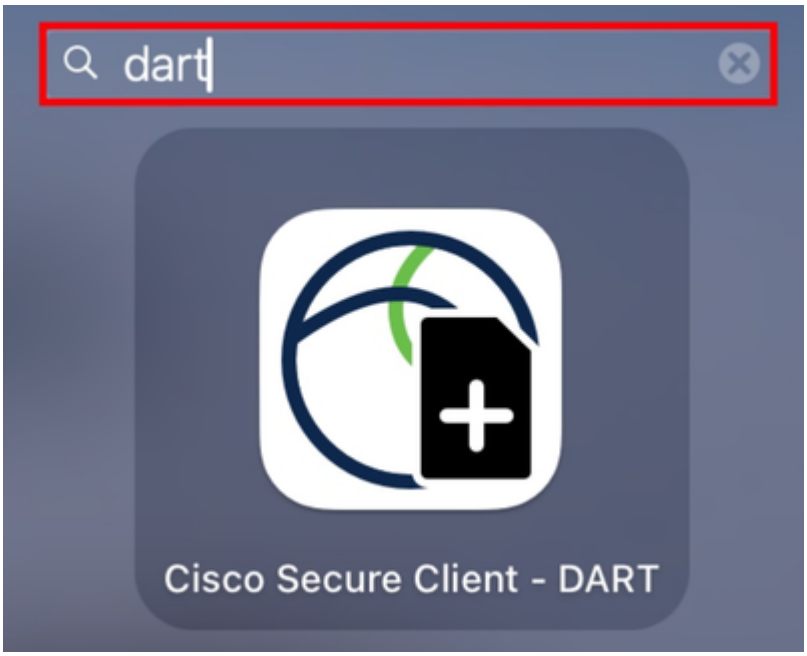
- Start Service

```
open -a "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app"
```

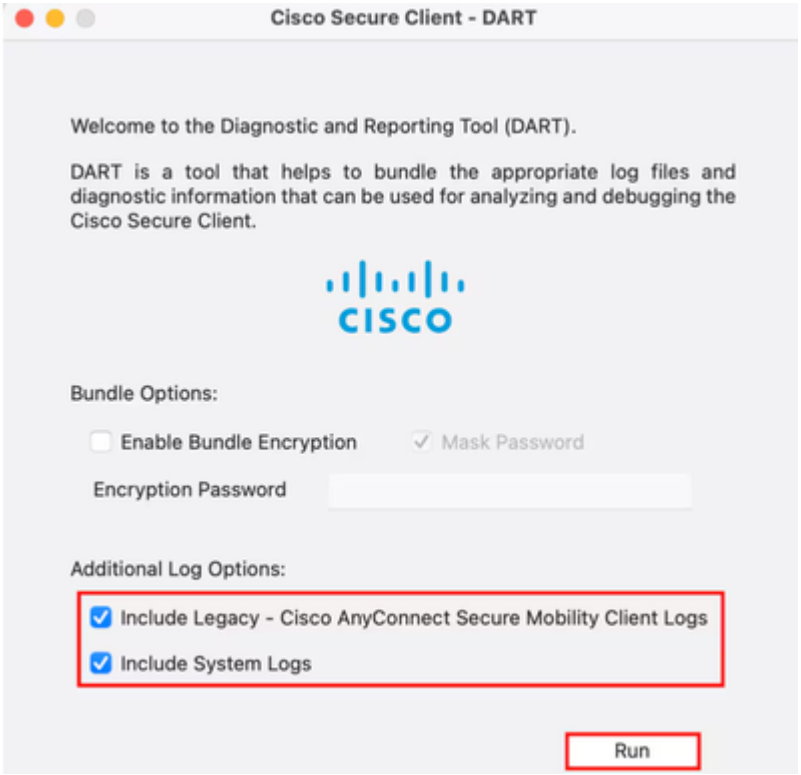
- 시작하기 Wireshark Capture
- 모든 인터페이스를 선택하고 패킷 캡처를 시작합니다



- 문제를 재현하고 저장KDF Logs 및Wireshark Capture다음 캡처할 단계를 수행합니다. DART Bundle
- 열기 Cisco Secure Client - DART



- 다음 옵션을 선택합니다.
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
  - Include System Logs
- 을 클릭합니다 Run



참고: 모든 로그, KDF 로그, Wireshark 캡처 및 DART 번들을 TAC 케이스에 수집합니다.

관련 정보

- Cisco 기술 지원 및 다운로드
- Cisco Secure Access Help Center
- Cisco ISE 설계 가이드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.