**Wireshark 사용법: HTTPS 트래픽 암호 해독**

**요약 보고서**

이 튜토리얼은 의심스러운 네트워크 활동을 조사하고 트래픽의 패킷 캡처(pcap)를 검토하는 보안 전문가를 위해 설계되었습니다. 이 설명서는 독자가 [**Wireshark**](https://www.wireshark.org/) 에 익숙하다고 가정하며 , Wireshark 버전 3.x를 중심으로 설명합니다.

의심스러운 네트워크 활동을 검토하다 보면 암호화된 트래픽을 발견하는 경우가 많습니다. 대부분의 웹사이트가 HTTPS(Hypertext Transfer Protocol Secure) 프로토콜을 사용하기 때문입니다. 하지만 대부분의 웹사이트처럼 다양한 종류의 악성 프로그램도 HTTPS를 사용합니다. 악성 프로그램 활동의 pcap 파일을 검토할 때 감염 후 트래픽에 어떤 내용이 포함되어 있는지 파악하는 것은 매우 유용합니다.

이 Wireshark 튜토리얼에서는 Wireshark를 사용하여 pcap 파일에서 HTTPS 트래픽을 복호화하는 방법을 설명합니다. 복호화는 pcap 파일이 처음 기록될 때 캡처된 암호화 키 데이터가 포함된 텍스트 기반 로그 파일을 통해 가능합니다. 이 키 로그 파일을 사용하면 pcap 파일의 HTTPS 활동을 복호화하고 내용을 검토할 수 있습니다.

[**오늘은 Dridex**](https://en.wikipedia.org/wiki/Dridex) 멀웨어 감염 시 발생하는 HTTPS 활동을 살펴보겠습니다 .

[**참고: 본 안내는 " Wireshark 사용자 지정 - 열 표시 변경**](https://unit42.paloaltonetworks.com/unit42-customizing-wireshark-changing-column-display/) " 에서 설명한 대로 Wireshark 열 표시를 사용자 지정했다고 가정합니다 .

[**다음은 이 튜토리얼에 사용된 pcap 파일과 주요 로그 파일이**](https://github.com/pan-unit42/wireshark-tutorial-decrypting-HTTPS-traffic) 포함된 ZIP 압축 파일이 있는 GitHub 저장소입니다 .

**경고 :** 이 튜토리얼에 사용된 pcap 파일에는 Windows 기반 악성코드가 포함되어 있습니다. Windows 컴퓨터를 사용하는 경우 감염 위험이 있습니다. 가능하면 BSD, Linux 또는 macOS와 같은 Windows 이외의 환경에서 이 pcap 파일을 검토하는 것이 좋습니다.

**암호화된 트래픽의 배경**

1990년대 중반부터 후반까지 웹사이트에서 가장 흔하게 사용되던 프로토콜은 암호화되지 않은 웹 트래픽을 생성하는 HTTP(Hypertext Transfer Protocol)였습니다. 그러나 보안에 대한 우려가 커지면서 웹사이트들은 HTTPS로 전환하기 시작했고, 이제 웹 브라우징에서 HTTP 트래픽을 사용하는 경우는 거의 찾아볼 수 없습니다.

HTTPS는 기본적으로 HTTP 트래픽을 포함하는 암호화된 통신 터널입니다. 이러한 터널은 처음에는 SSL(Secure Sockets Layer)을 암호화 프로토콜로 사용했습니다. 오늘날 대부분의 HTTPS 트래픽은 TLS(Transport Layer Security)를 사용합니다.

**HTTPS 웹 트래픽**

HTTPS 트래픽은 종종 도메인 이름을 보여줍니다. 예를 들어, 웹 브라우저에서 https://www.wireshark.org를 볼 때, [**Wireshark의 사용자 지정 열 표시**](https://unit42.paloaltonetworks.com/unit42-customizing-wireshark-changing-column-display/) 에서 pcap 파일을 보면 해당 트래픽의 서버 이름이 www.wireshark.org 로 표시됩니다 . 하지만 실제 URL이나 서버에서 반환된 데이터와 같은 다른 세부 정보는 알 수 없습니다. pcap 파일의 TCP(Transmission Control Protocol) 스트림을 추적해도 해당 트래픽의 내용은 암호화되어 있기 때문에 확인할 수 없습니다.

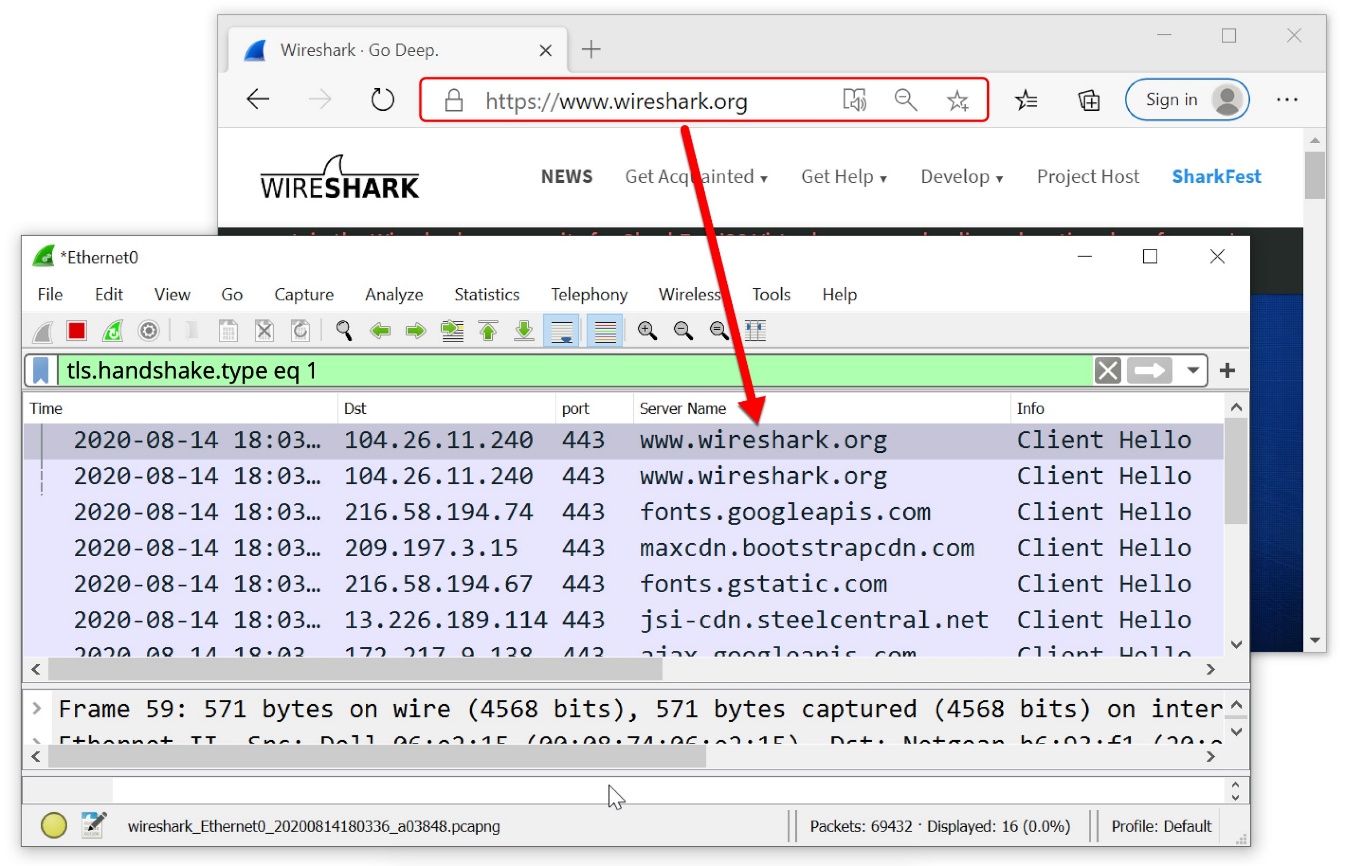
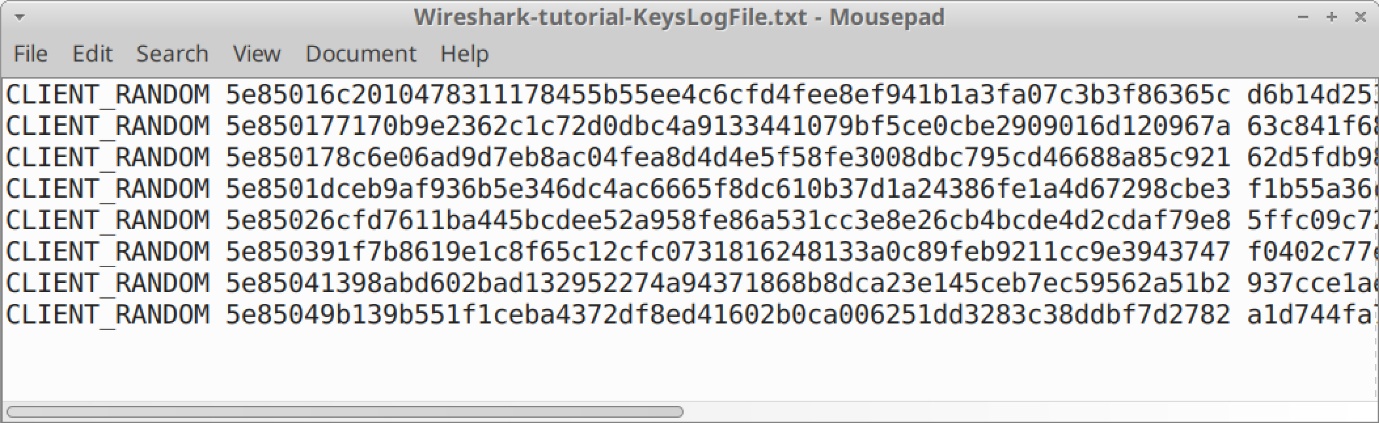
그림 1. HTTPS 트래픽에서 www.wireshark.org로의 트래픽.

그림 2. www.wireshark.org 서버와의 HTTPS 트래픽 TCP 스트림.

**암호화 키 로그 파일**

암호화 키 로그는 텍스트 파일입니다. 그림 3에 예시가 나와 있습니다.

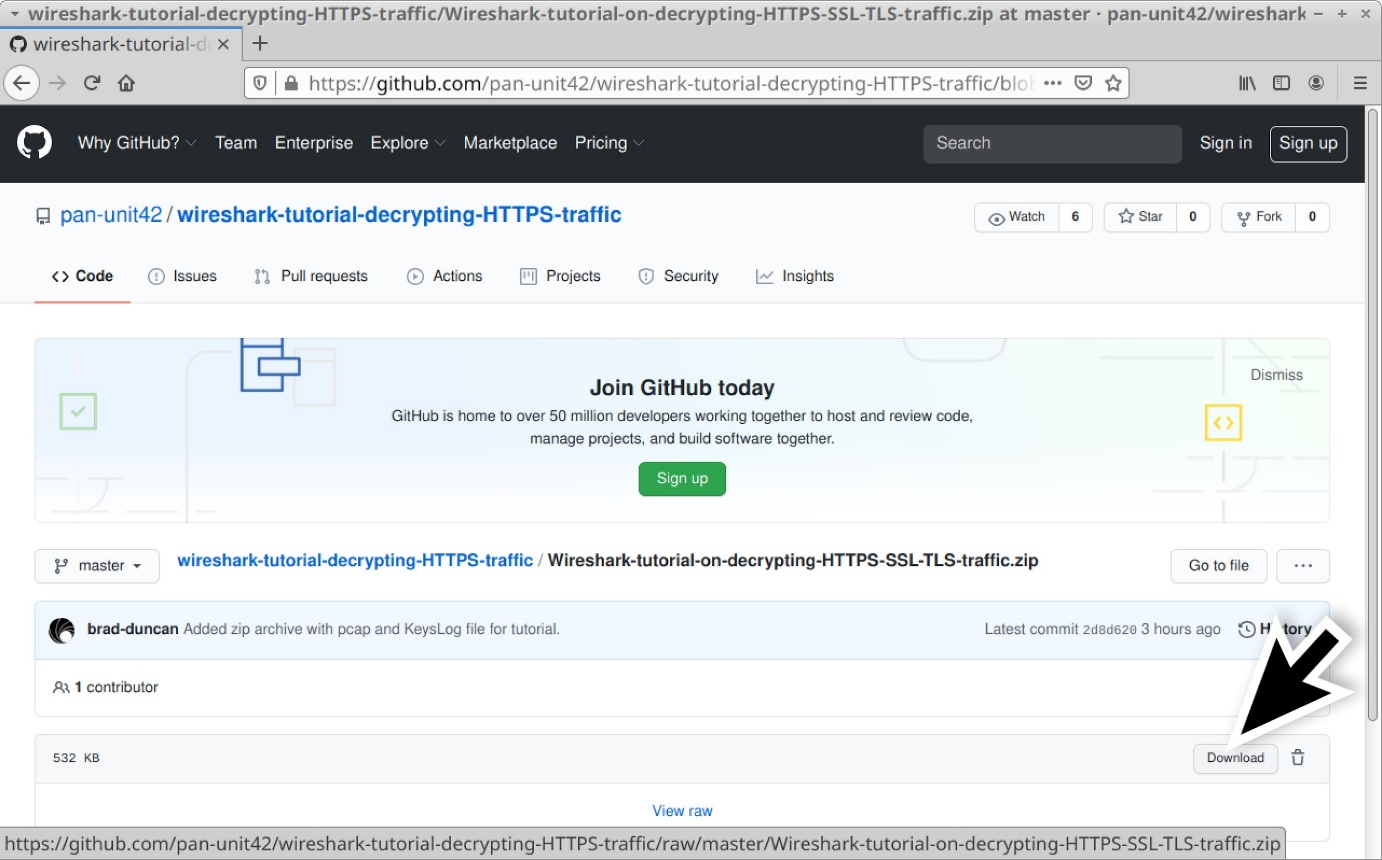
그림 3. 이 튜토리얼에서 사용된 주요 로그 파일.

이 로그 파일은 pcap 파일이 처음 기록될 때 중간자 공격(MitM) 기법을 사용하여 생성됩니다. pcap 파일 기록 시 이러한 파일이 생성되지 않은 경우 해당 pcap 파일의 HTTPS 트래픽을 복호화할 수 없습니다.

**키 로그 파일이 포함된 Pcap 예시**

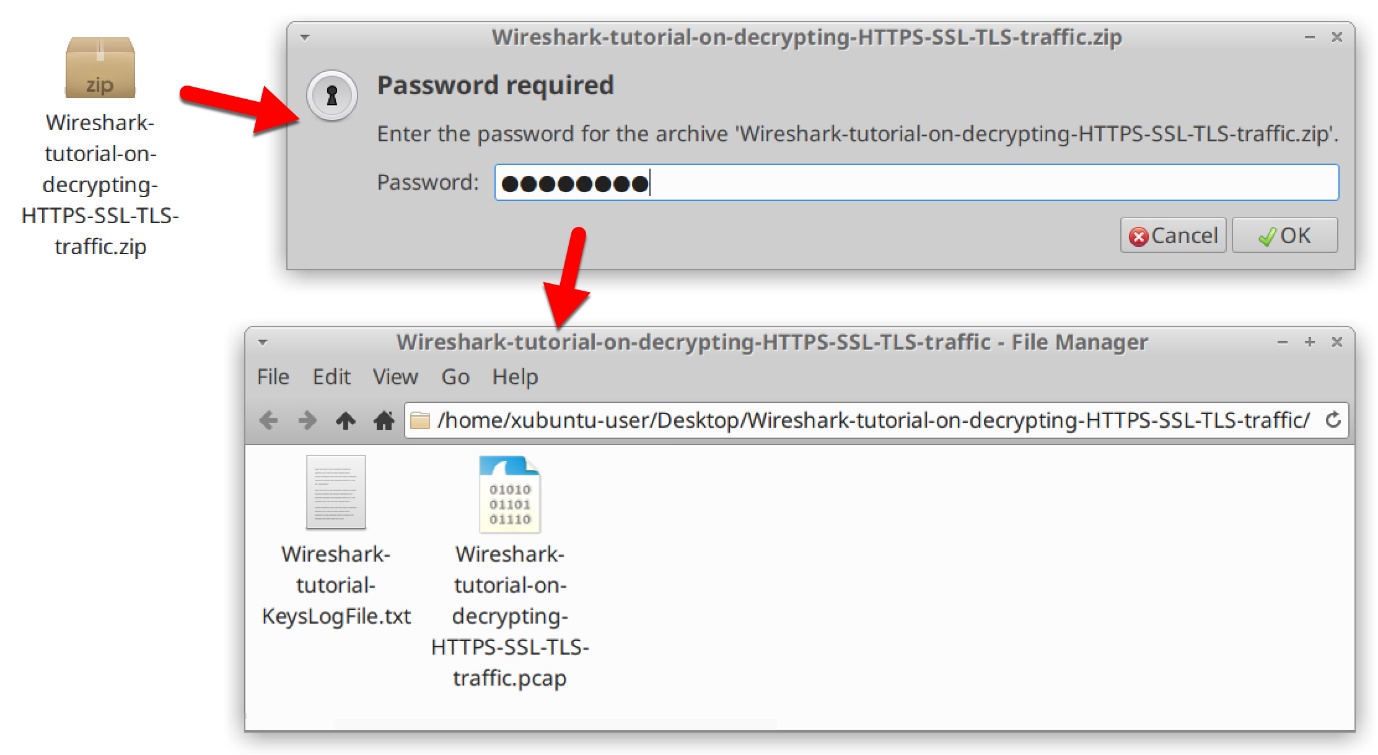
pcap 파일과 키 로그 파일이 포함된 암호로 보호된 ZIP 압축 파일은 [**이 GitHub 저장소**](https://github.com/pan-unit42/wireshark-tutorial-decrypting-HTTPS-traffic) 에서 다운로드할 수 있습니다 . GitHub 페이지로 이동하여 ZIP 압축 파일 항목을 클릭한 다음 그림 4와 5에 표시된 대로 다운로드하십시오. 참고로, 이 ZIP 압축 파일에 포함된 pcap 파일은 키 로그를 사용하여 복호화하면 Windows 기반 악성코드 샘플에 접근할 수 있습니다. 항상 그렇듯이 주의를 기울여 Windows 환경이 아닌 환경에서 이 튜토리얼의 단계를 따르시기 바랍니다.

그림 4. 이 튜토리얼에 사용된 ZIP 압축 파일 링크가 포함된 GitHub 저장소.

그림 5. 이 튜토리얼의 ZIP 압축 파일을 다운로드하는 모습.

***"infected"를*** 암호로 사용하여 ZIP 압축 파일에서 pcap 및 키 로그 파일을 추출하십시오. 그러면 그림 6과 같이 두 개의 파일이 생성됩니다.

* Wireshark 튜토리얼 키 로그 파일.txt
* Wireshark를 이용한 HTTPS-SSL-TLS 트래픽 해독 튜토리얼.pcap

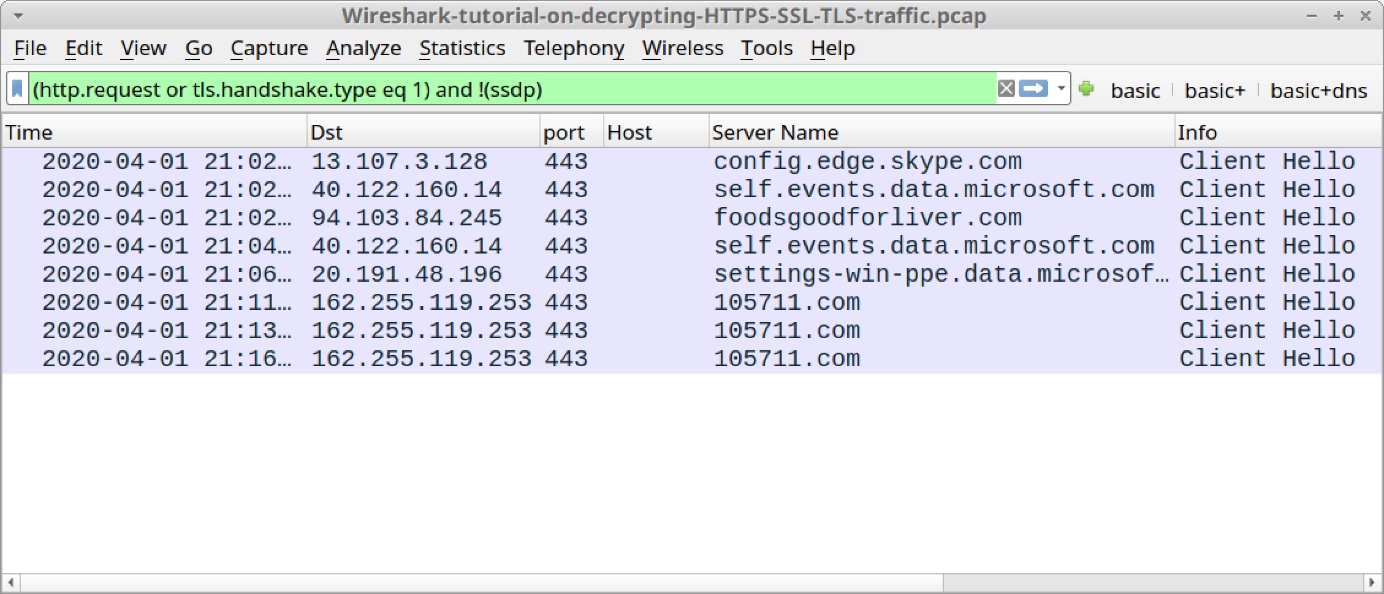
그림 6. 이 튜토리얼의 주요 로그 파일 및 pcap 파일.

**키 로그 파일 없이 HTTPS 트래픽**

***Wireshark에서 Wireshark-tutorial-on-decrypting-HTTPS-SSL-TLS-traffic.pcap 파일을*** 엽니다 . 이전 [**Wireshark 필터 관련 튜토리얼**](https://unit42.paloaltonetworks.com/using-wireshark-display-filter-expressions/) 에서 설명한 대로 기본 웹 필터를 사용합니다 . Wireshark 3.x용 기본 필터는 다음과 같습니다.

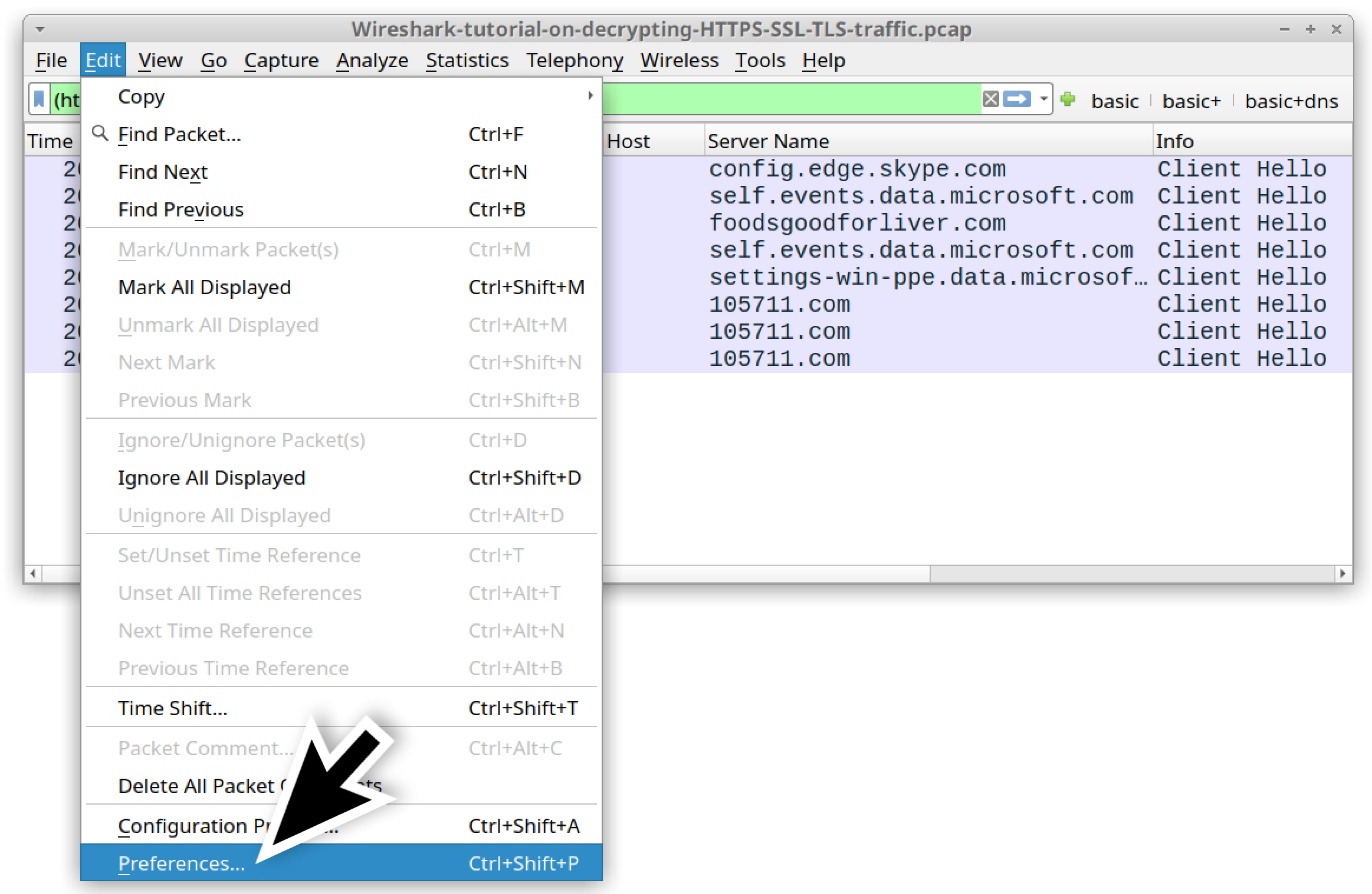
(http.request 또는 tls.handshake.type이 1과 같음) 및 !(ssdp)

이 pcap 파일은 Windows 10 호스트에서 발생한 Dridex 악성코드 감염의 결과입니다. 감염 활동을 포함한 모든 웹 트래픽은 HTTPS를 사용합니다. 핵심 로그 파일이 없으면 그림 7에서처럼 IP 주소, TCP 포트 및 도메인 이름만 확인할 수 있을 뿐 트래픽에 대한 자세한 내용은 알 수 없습니다.

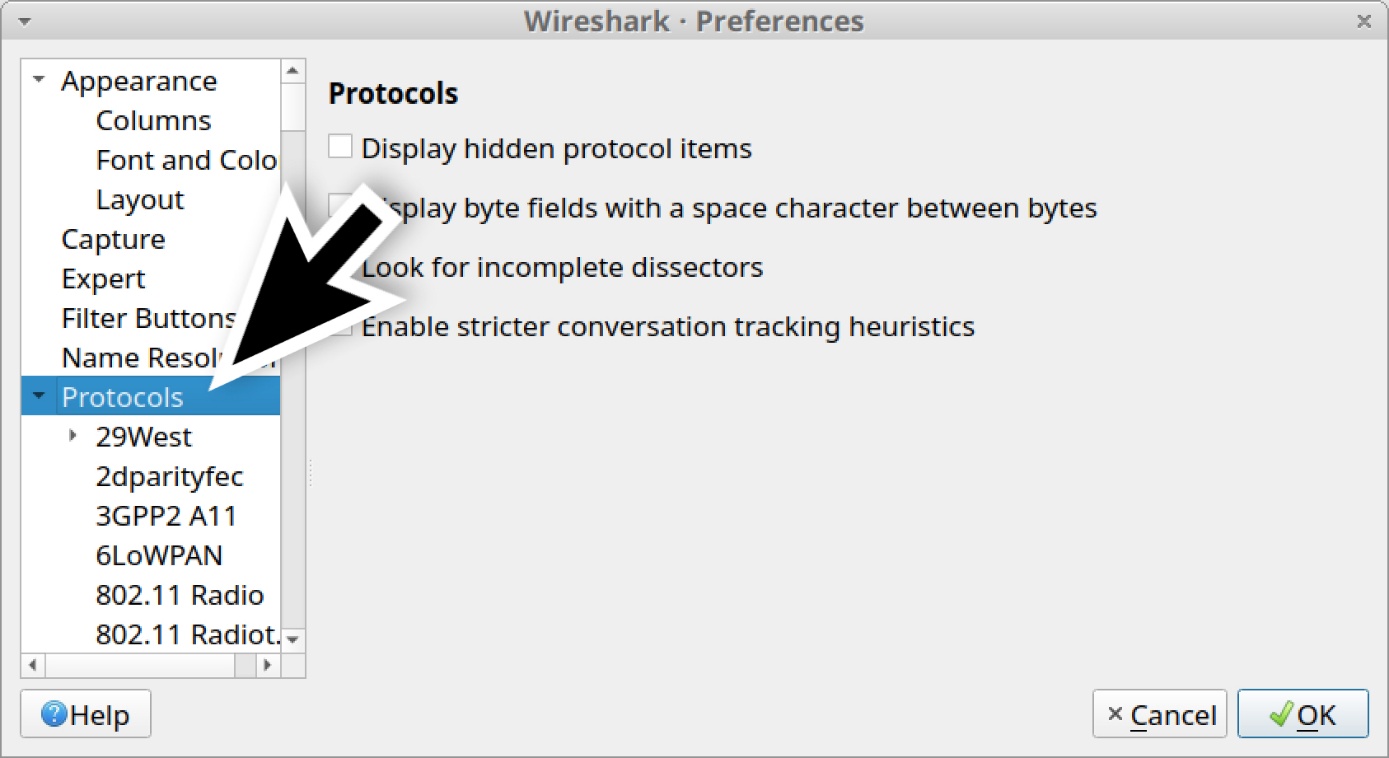
그림 7. 암호 해독 없이 기본 웹 필터를 사용하여 Wireshark에서 pcap 파일을 보는 모습.

**키 로그 파일 로드 중**

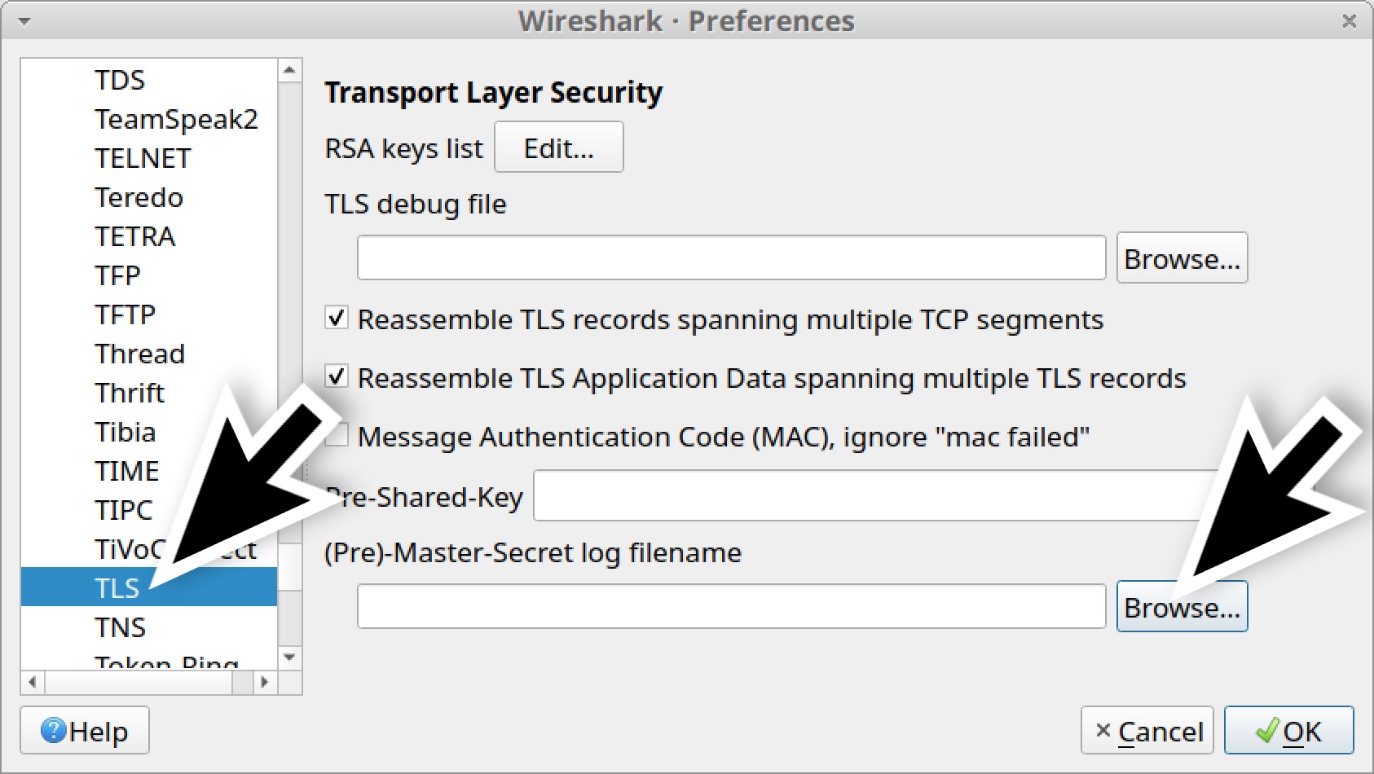
Wireshark에서 ***Wireshark-tutorial-on-decrypting-HTTPS-SSL-TLS-traffic.pcap 파일을*** 엽니다 . 그런 다음 그림 8과 같이 ***[편집] --> [환경 설정]*** 메뉴 경로를 사용하여 환경 설정 메뉴를 엽니다.

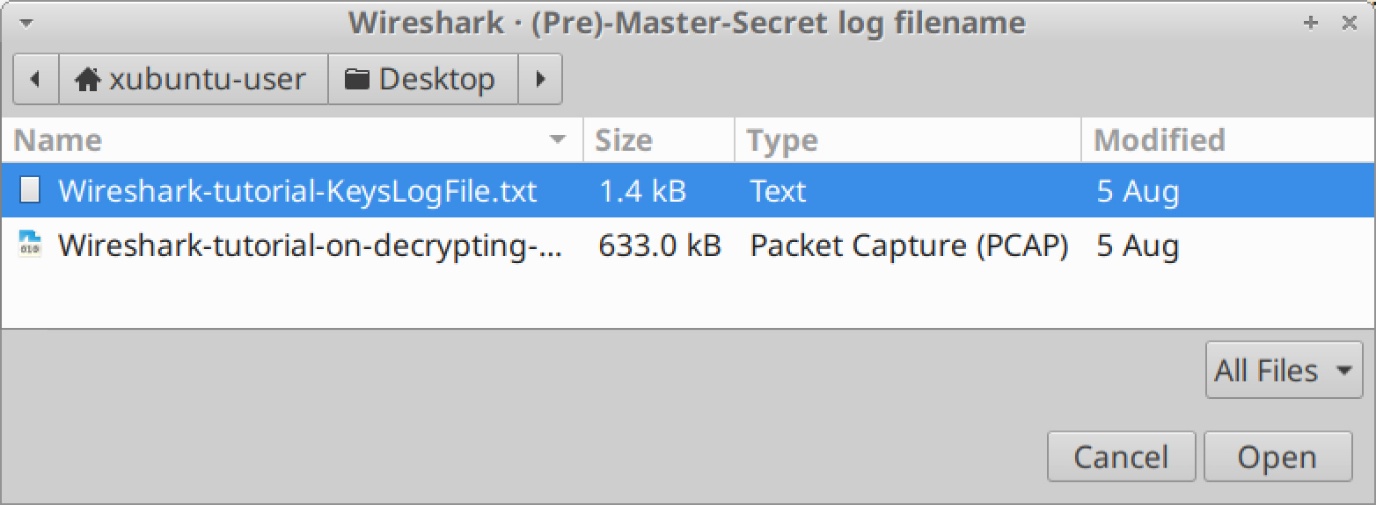
그림 8. Wireshark에서 환경설정 메뉴에 접근하는 방법.

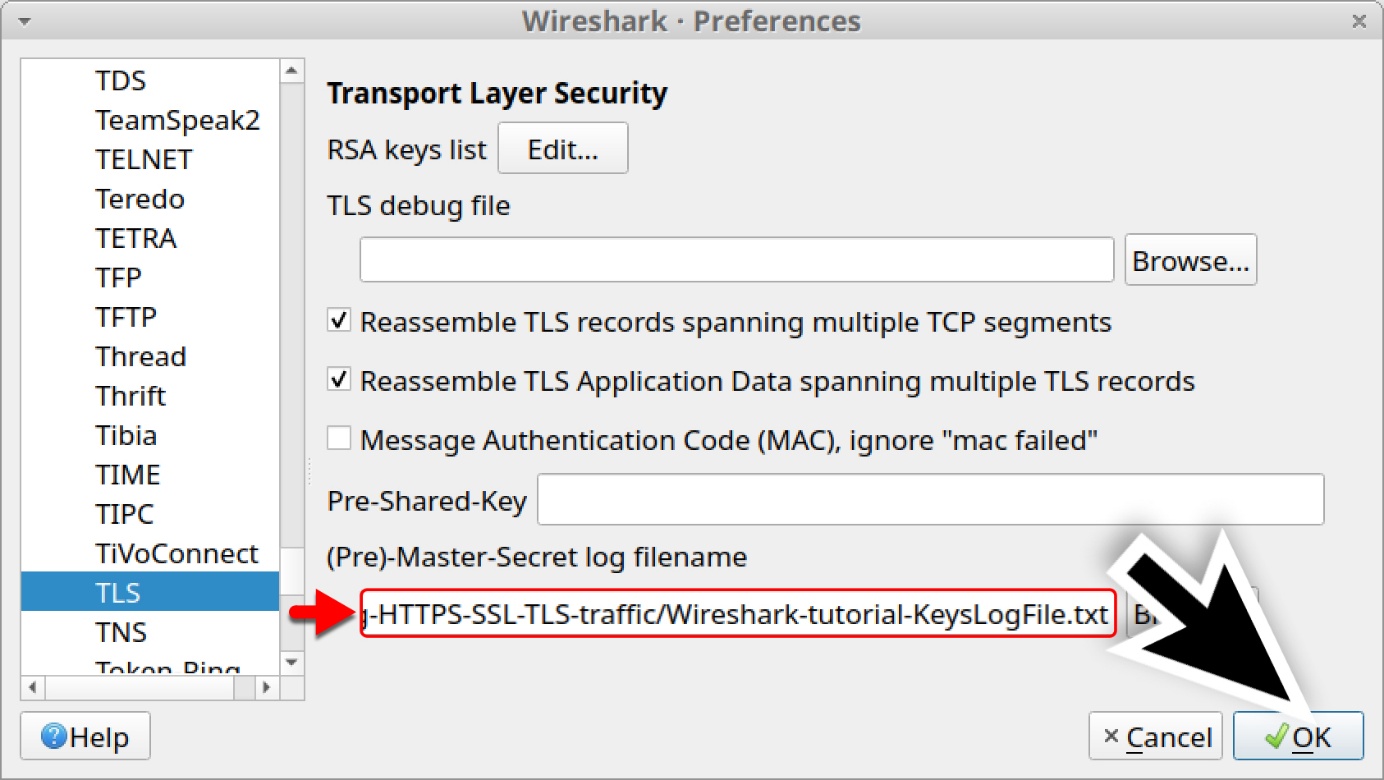
환경설정 메뉴의 왼쪽에서 그림 9와 같이 프로토콜을 클릭합니다.

그림 9. 환경설정 메뉴에서 프로토콜 선택.

Wireshark 2.x 버전을 사용 중인 경우, 아래로 스크롤하여 ***SSL을*** 찾아 선택하십시오. Wireshark 3.x 버전을 사용 중인 경우, 아래로 스크롤하여 ***TLS를*** 찾아 선택하십시오. SSL 또는 TLS를 선택하면 ***(Pre)-Master-Secret 로그 파일 이름*** 이라는 줄이 표시됩니다 . "찾아보기" 버튼을 클릭하고 그림 10, 11, 12에 표시된 것처럼 ***Wireshark-tutorial-KeysLogFile.txt 라는 키 로그 파일을 선택하십시오.***

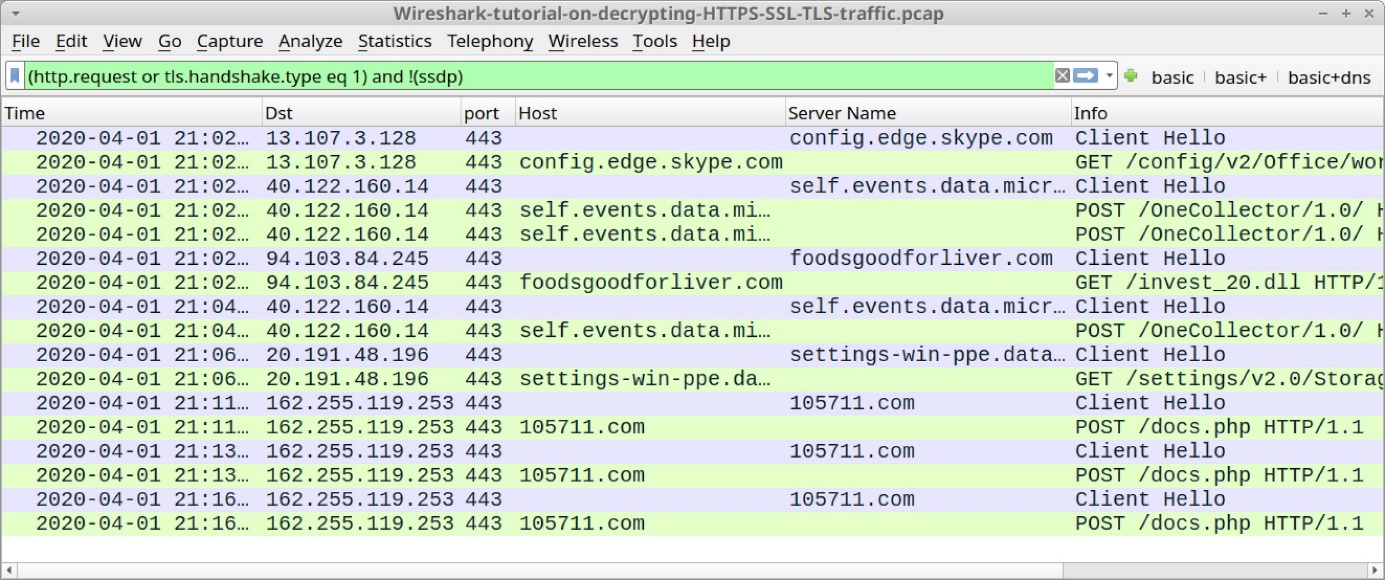
그림 10. Wireshark 3.x에서 TLS 아래의 (Pre)-Master-Secret 로그 파일 이름 필드를 찾는 방법.

그림 11. 이 튜토리얼에 사용할 주요 로그 파일 선택.

그림 12. (사전)마스터 시크릿 로그 파일 이름으로 파일을 선택했으면 "확인"을 클릭합니다.

**HTTPS 트래픽과 주요 로그 파일**

기본 필터를 사용할 때 "확인"을 클릭하면 그림 13과 같이 Wireshark 열 표시에서 각 HTTPS 라인 아래에 복호화된 HTTP 요청이 나열됩니다.

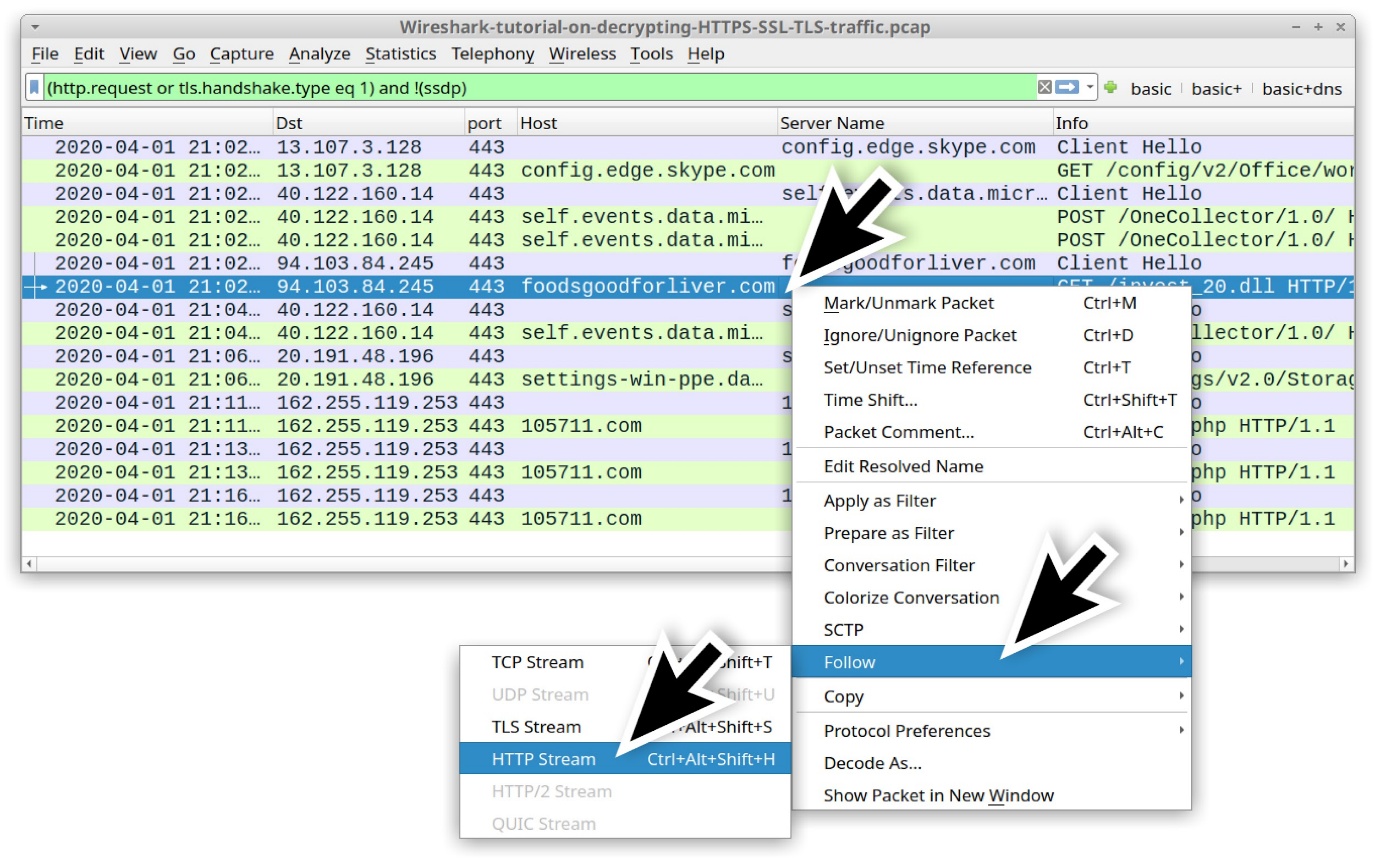
그림 13. 키 로그 파일을 사용한 후 Wireshark에서 HTTPS 복호화 결과.

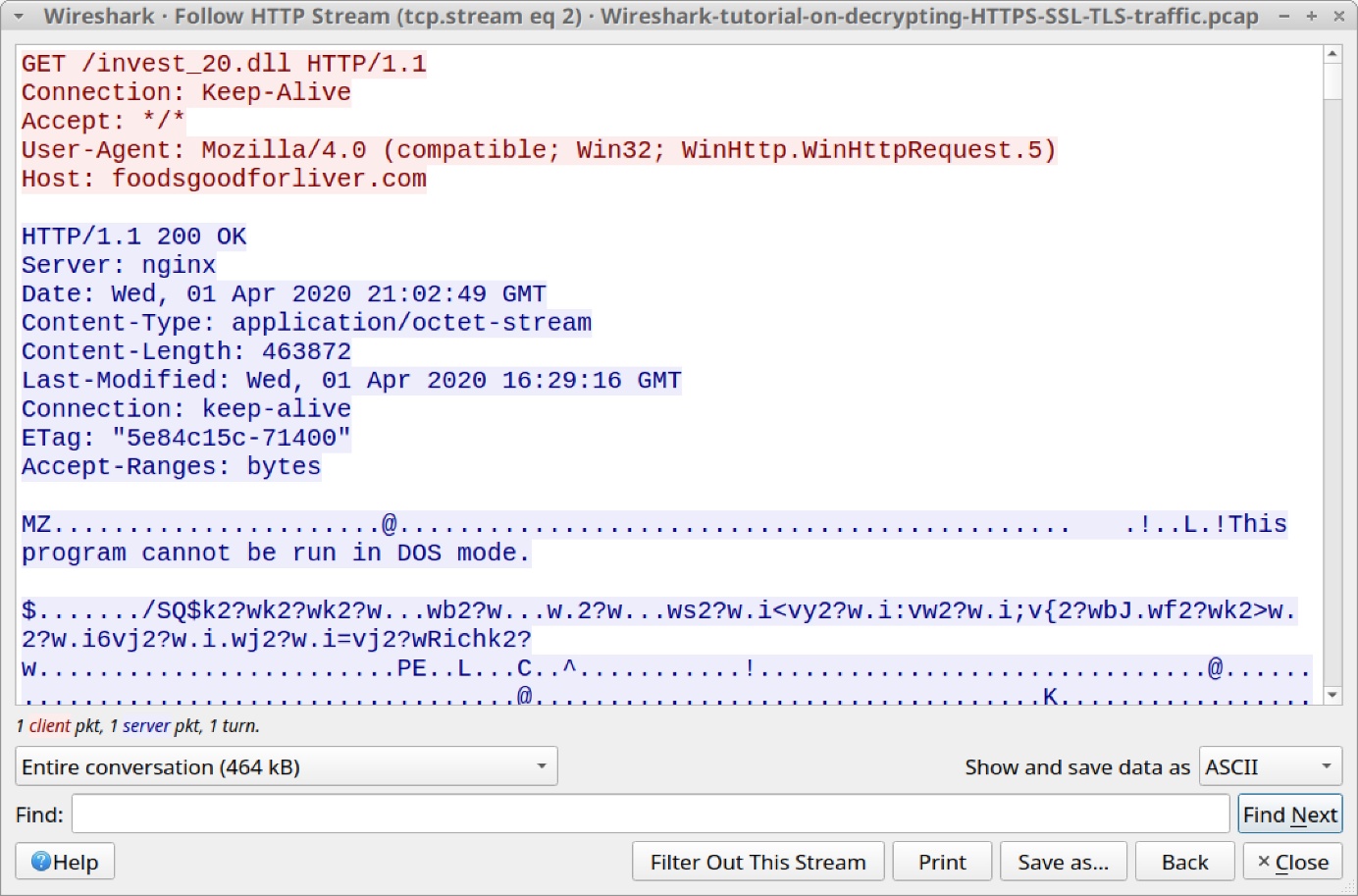
이 pcap 파일에서 이전에는 HTTPS 트래픽에 숨겨져 있던 microsoft.com 및 skype.com 도메인 에 대한 HTTP 요청을 확인할 수 있습니다 . 또한 Dridex 감염으로 인해 발생한 다음과 같은 트래픽도 발견했습니다.

* foodsgoodforliver[.]com - GET /invest\_20.dll
* 105711[.]com - POST /docs.php

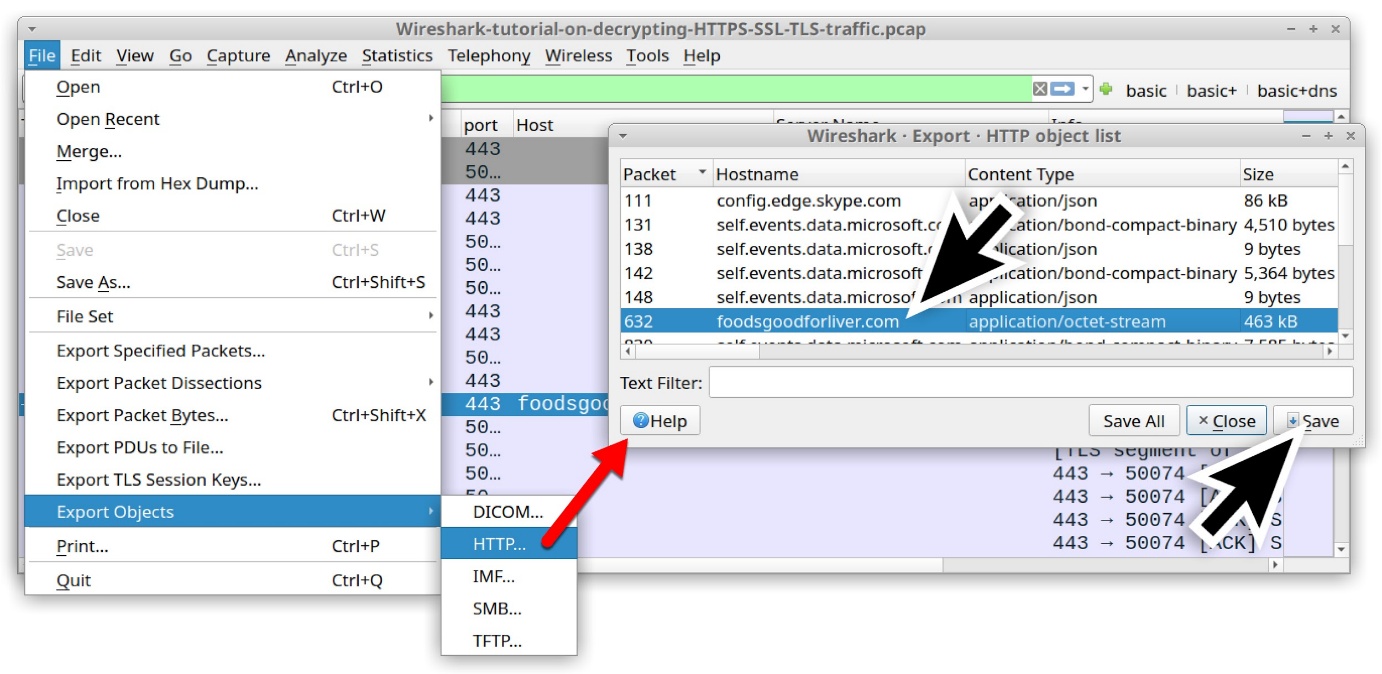
foodsgoodforliver[.]com 에 대한 GET 요청은 Dridex용 DLL 파일을 반환했습니다. 105711[.]com 에 대한 POST 요청은 Dridex에 감염된 Windows 호스트에서 발생하는 명령 및 제어(C2) 트래픽입니다.

HTTP 스트림을 따라가면 트래픽을 검토할 수 있습니다. 해당 줄을 마우스 오른쪽 버튼으로 클릭하여 선택한 다음 마우스 왼쪽 버튼으로 클릭하여 HTTP 스트림을 따라갈 수 있는 메뉴를 불러옵니다. 그림 14와 15는 foodsgoodforliver[.]com 에 대한 HTTP GET 요청의 HTTP 스트림을 따라가는 것을 보여줍니다 .

그림 14. foodsgoodforliver[.]com에 대한 GET 요청의 HTTP 스트림을 보여줍니다.

그림 15. HTTP 스트림은 서버에서 반환된 EXE 또는 DLL을 나타냅니다.

이제 해당 트래픽에 대한 주요 로그 파일을 확보했으므로 pcap 파일에서 이 악성코드를 내보낼 수 있습니다. 그림 16과 같이 메뉴 경로 [ ***파일] > [개체 내보내기] > [HTTP]를*** 사용하여 pcap 파일에서 이 파일을 내보냅니다.

그림 16. foodsgoodforliver[.]com에서 반환된 악성코드 바이너리를 내보내는 모습.

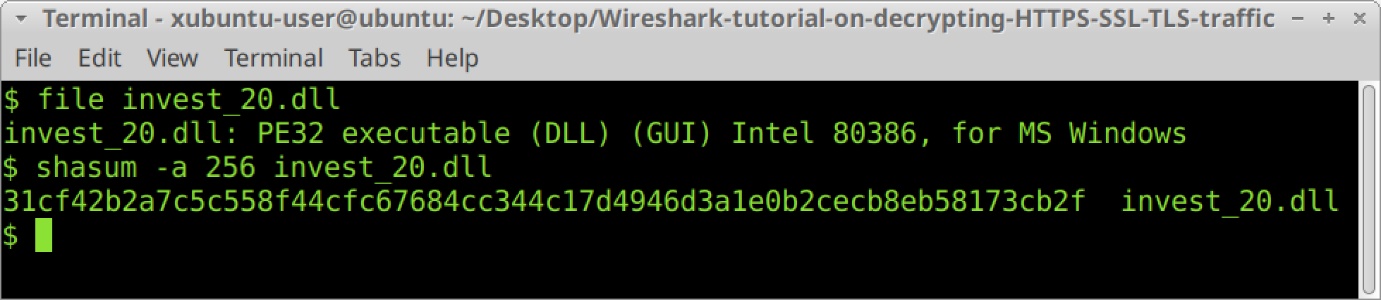
BSD, Linux 또는 macOS 환경을 사용 중인 경우 터미널 창을 열고 다음 명령어를 사용하십시오.

파일

이 파일이 DLL 파일인지 확인하는 명령어를 사용하세요. 그런 다음 사용하세요.

샤숨 -a 256

그림 17에 표시된 것처럼 파일의 SHA256 해시값을 얻습니다.

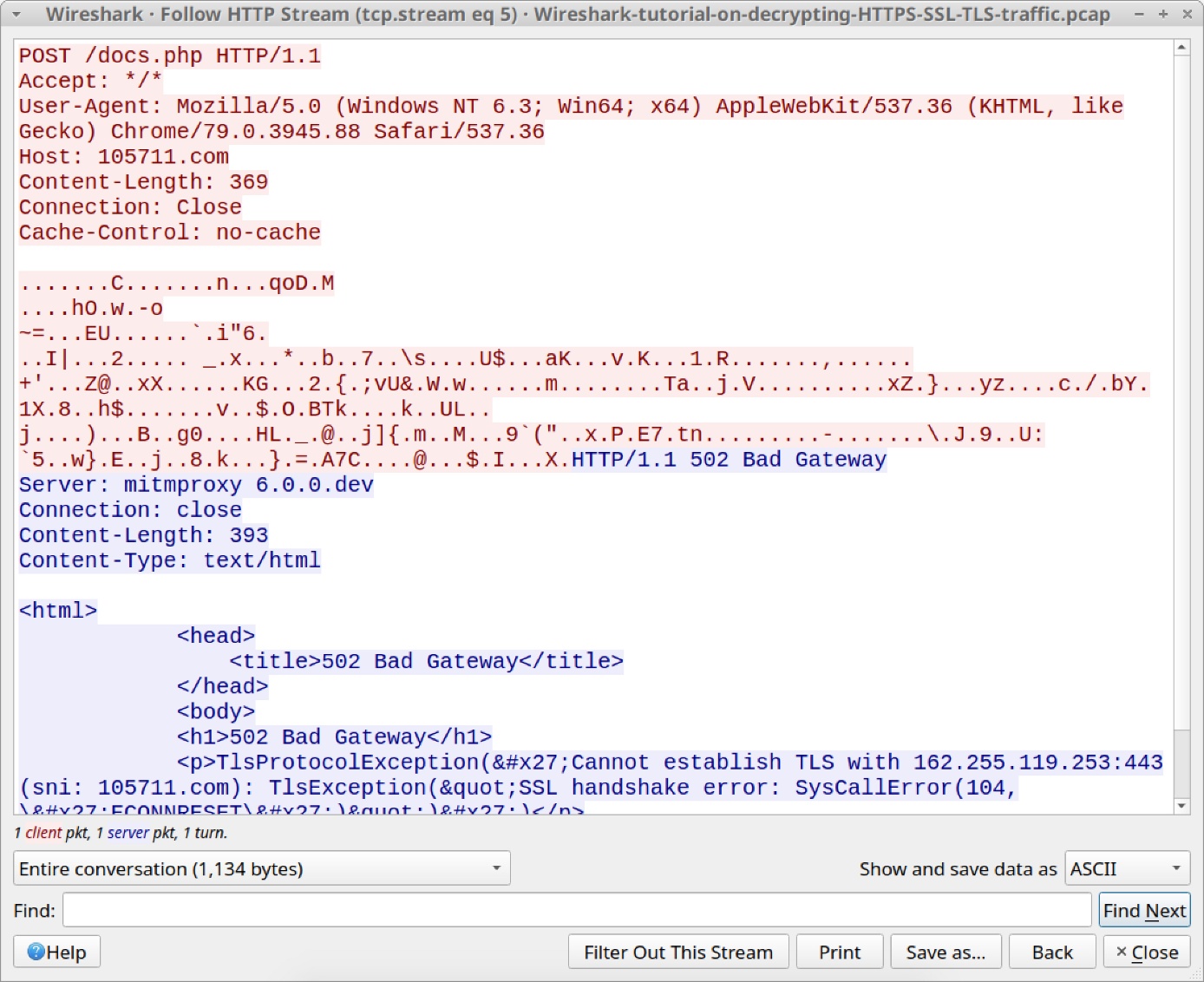
그림 17. 리눅스 환경에서 이 악성코드의 SHA256 해시값을 얻는 방법.

이 악성코드의 SHA256 해시는 다음과 같습니다.

31cf42b2a7c5c558f44cfc67684cc344c17d4946d3a1e0b2cecb8eb58173cb2f

[**이 해시값을 온라인에서 검색**](https://www.google.com/search?q=31cf42b2a7c5c558f44cfc67684cc344c17d4946d3a1e0b2cecb8eb58173cb2f) 하면 최소한 두 곳의 공개된 온라인 샌드박스 환경에서 결과를 찾을 수 있을 것입니다.

마지막으로, 이 Dridex 감염에서 발생한 C2 트래픽을 검토할 수 있습니다. 기본 웹 필터를 사용한 다음, 105711[.]com 으로 전송된 POST 요청 중 하나에서 HTTP 스트림을 따라가 보세요 . 그림 18은 HTTP 스트림의 예시를 보여줍니다.

그림 18. Dridex C2 POST 요청 중 하나의 HTTP 스트림.

**결론**

이 튜토리얼에서는 키 로그 텍스트 파일을 사용하여 Wireshark로 pcap 파일의 HTTPS 트래픽을 복호화하는 방법을 살펴보았습니다. pcap 파일을 처음 녹화할 때 생성된 키 로그 파일이 없으면 Wireshark에서 해당 pcap 파일의 HTTPS 트래픽을 복호화할 수 없습니다.