Wireshark Network Analysis: Full Workflow Documentation

This document provides a detailed walkthrough of network packet capture and analysis performed using Wireshark. It breaks down each major stage as part of a cybersecurity investigation workflow, suitable for inclusion in a CV, portfolio, or GitHub case study.

1. Launching Wireshark & Selecting an Interface

The process begins by opening Wireshark and selecting a network interface to monitor. This step is crucial as selecting the wrong interface would lead to incomplete or irrelevant traffic capture.

2. Starting the Packet Capture

Once the interface is selected, packet capture begins. Wireshark starts logging real-time network activity, displaying packets by protocol, source, destination, and size.

3. Filtering Traffic for Analysis

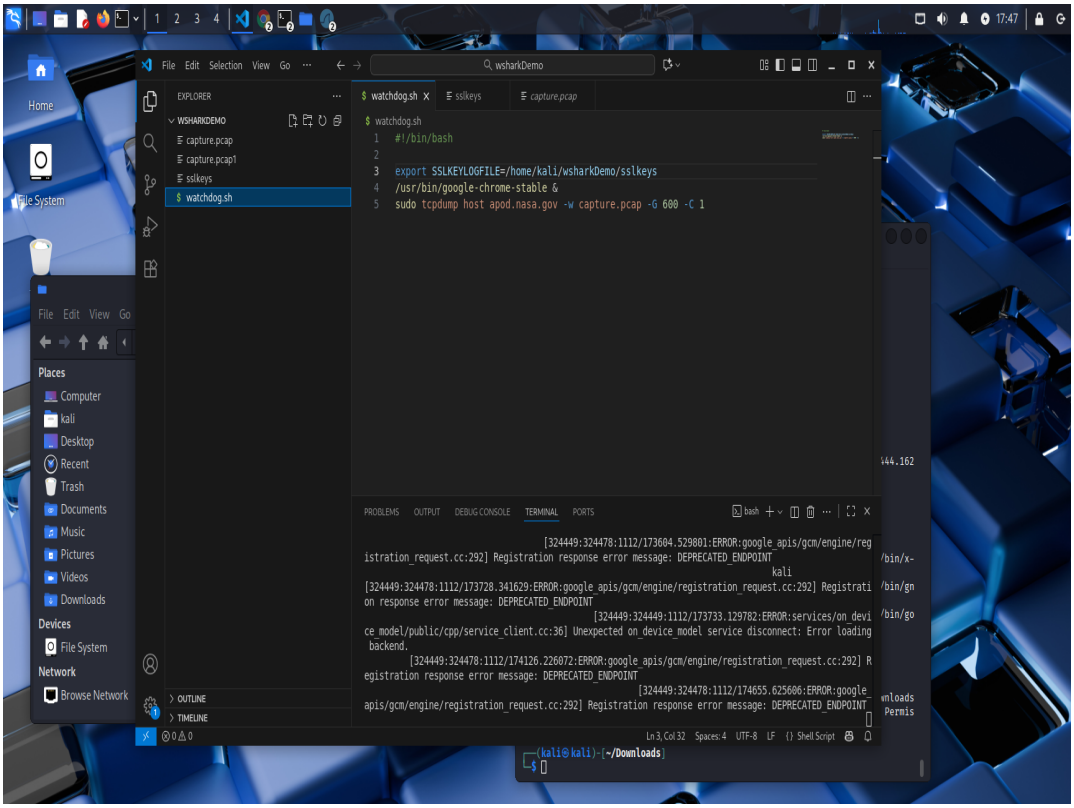
Filters are applied to isolate relevant packets. For example, filtering by protocol (e.g., HTTP, DNS, TCP) allows targeted investigation and reduces noise.

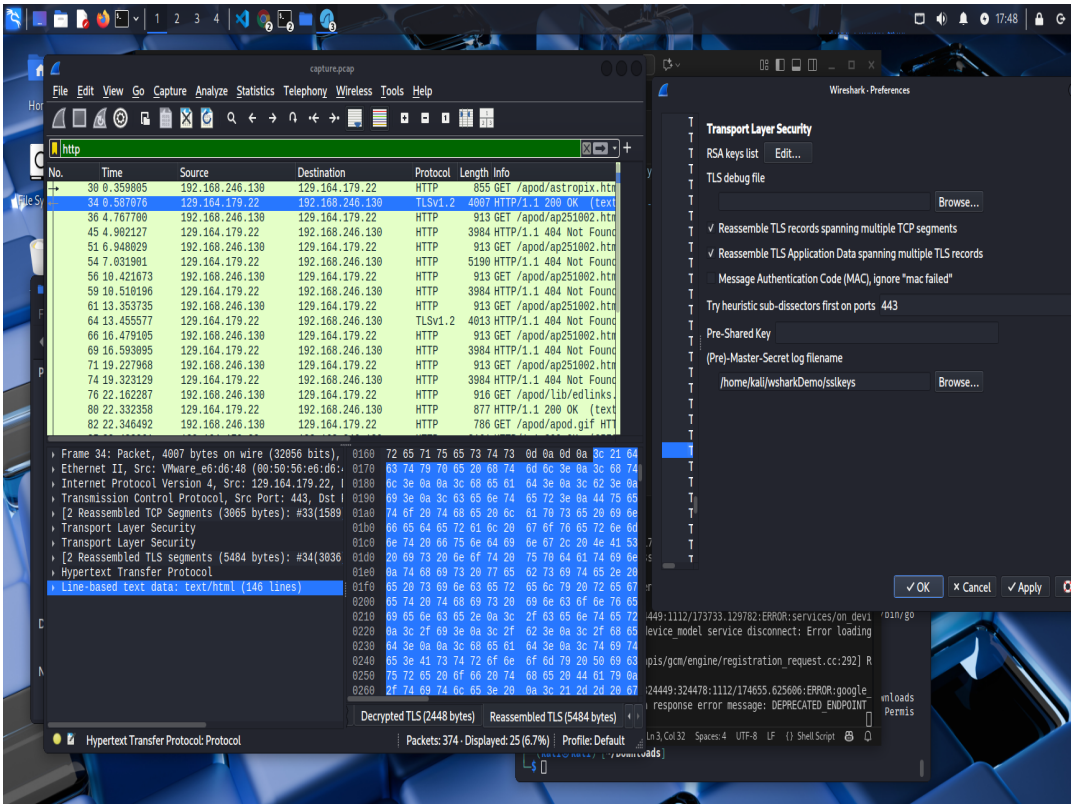
4. Inspecting Individual Packets

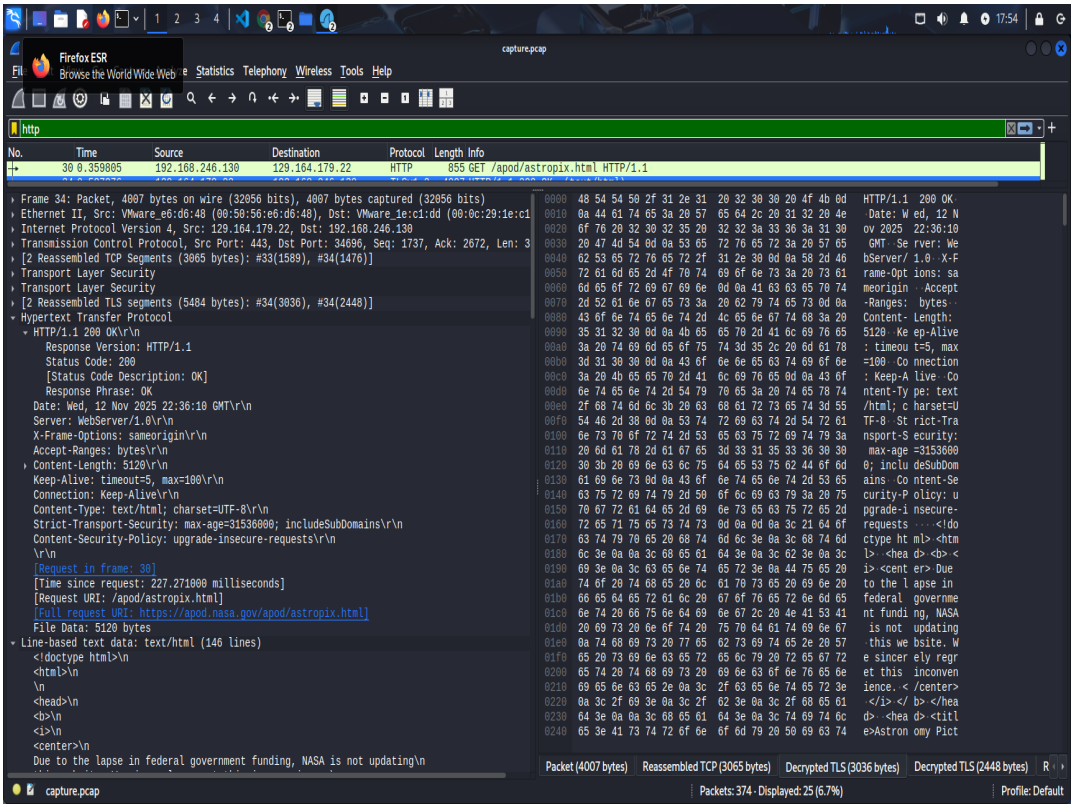
Packets are examined in detail to explore headers, payloads, flags, timestamps, and communication flows. This stage is essential for detecting anomalies or suspicious behaviours.

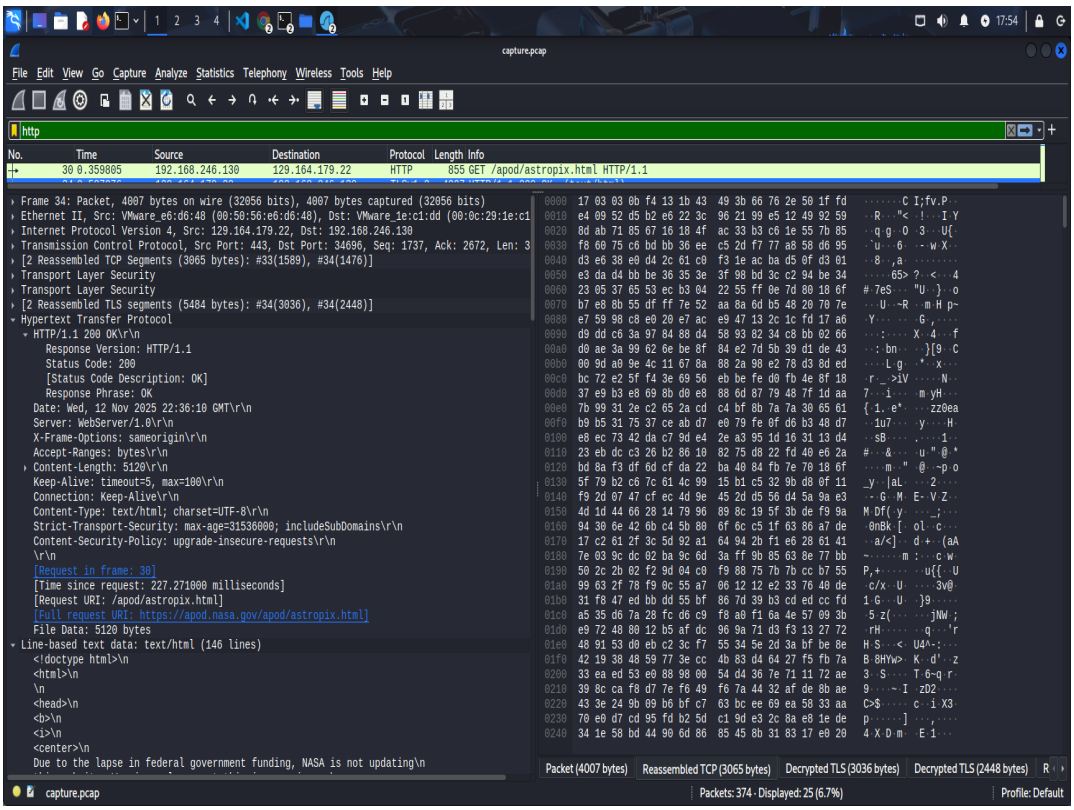
5. Exporting Results & Final Report

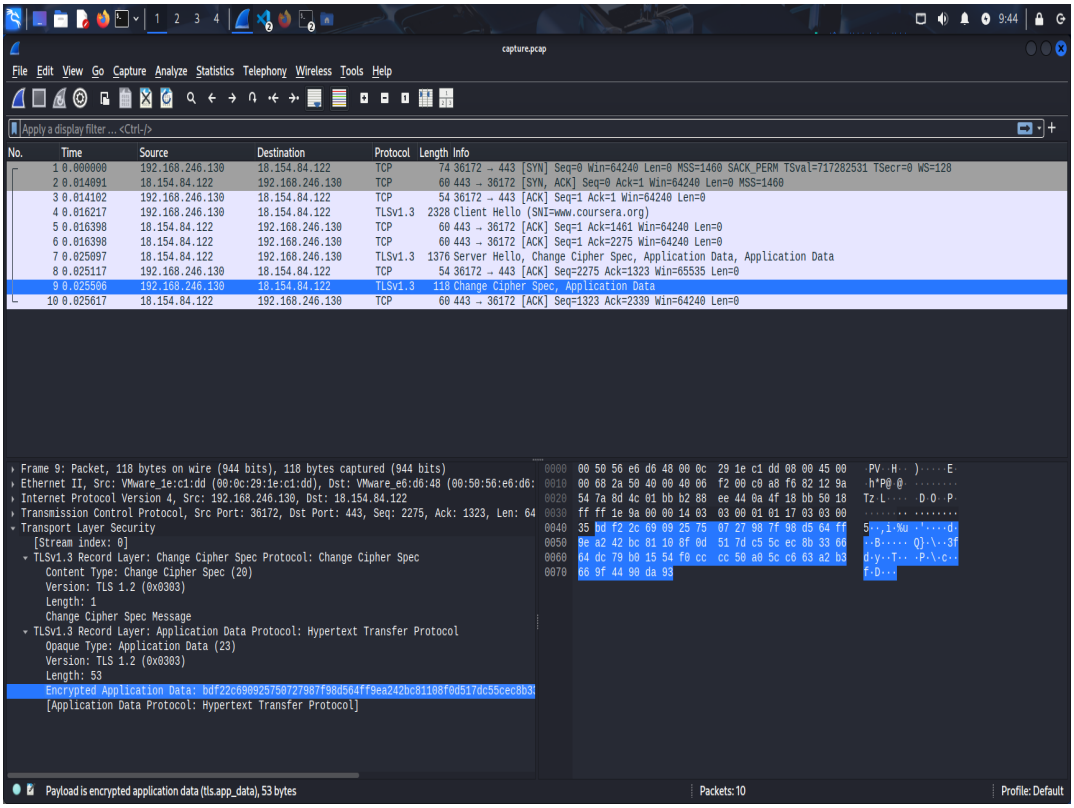
The capture is exported or saved, and findings are summarised for reporting or incident response.

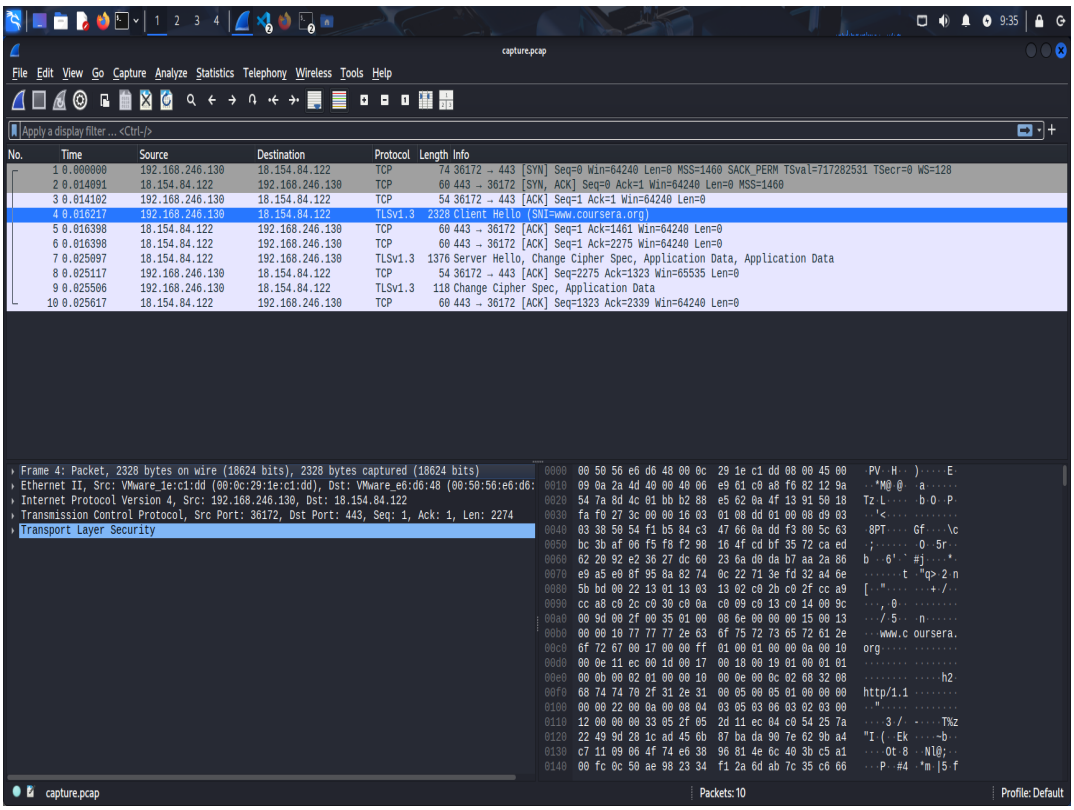

wsharkDemo
watchdog.sh
sslkeys
capture.pcap
capture.pcap1
#!/bin/bash
export SSLKEYLOGFILE=/home/kali/wsharkDemo/sslkeys
/usr/bin/google-chrome-stable &
sudo tcpdump host apod.nasa.gov -w capture.pcap -G 600 -C 1
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
[324449:324478:1112/173604.529801:ERROR:google_apis/gcm/engine/registration_request.cc:292] Registration response error message: DEPRECATED_ENDPOINT
[324449:324478:1112/173728.341629:ERROR:google_apis/gcm/engine/registration_request.cc:292] Registration response error message: DEPRECATED_ENDPOINT
[324449:324449:1112/173733.129782:ERROR:services/on_device_model/public/cpp/service_client.cc:36] Unexpected on_device_model service disconnect: Error loading backend.
[324449:324478:1112/174126.226072:ERROR:google_apis/gcm/engine/registration_request.cc:292] Registration response error message: DEPRECATED_ENDPOINT
[324449:324478:1112/174655.625606:ERROR:google_apis/gcm/engine/registration_request.cc:292] Registration response error message: DEPRECATED_ENDPOINT
(kali@kali)-[~/Downloads]

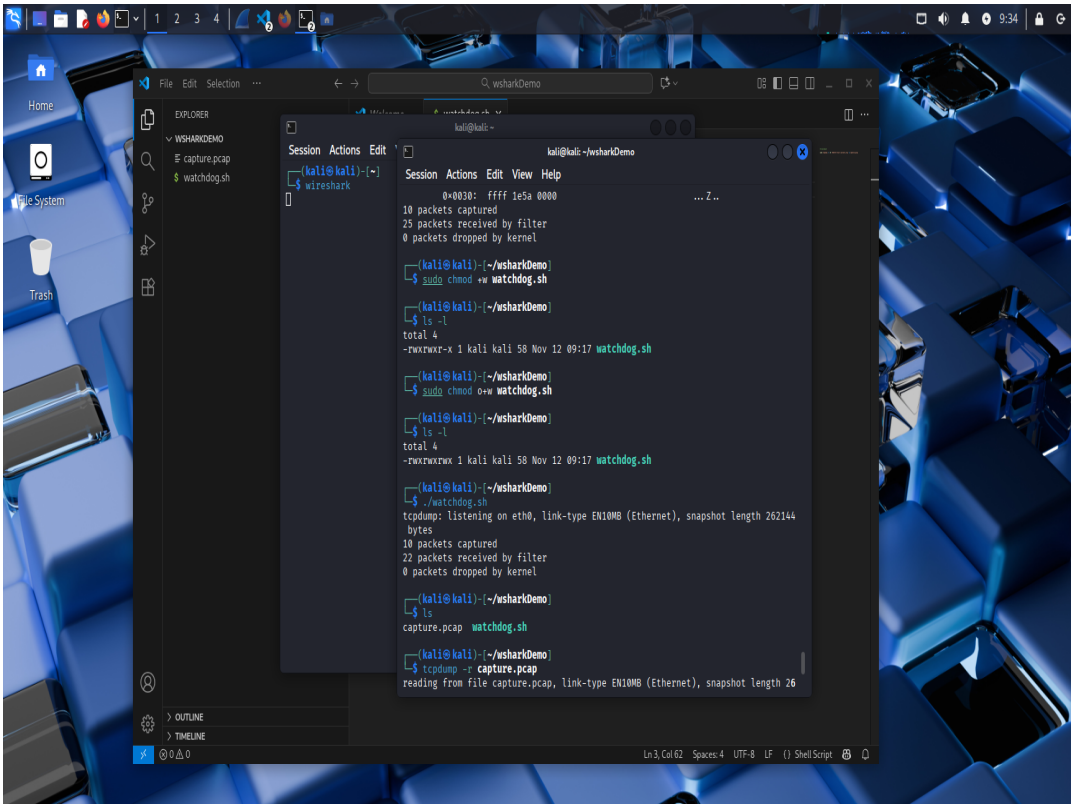

capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
30 0.359805 192.168.246.130 129.164.179.22 HTTP 855 GET /apod/astropix.html
34 0.587076 129.164.179.22 192.168.246.130 TLSv1.2 4007 HTTP/1.1 200 OK (text
36 4.767700 192.168.246.130 129.164.179.22 HTTP 913 GET /apod/ap251002.html
45 4.902127 129.164.179.22 192.168.246.130 HTTP 3984 HTTP/1.1 404 Not Found
51 6.948029 192.168.246.130 129.164.179.22 HTTP 913 GET /apod/ap251002.html
54 7.031901 129.164.179.22 192.168.246.130 HTTP 5190 HTTP/1.1 404 Not Found
56 10.421673 192.168.246.130 129.164.179.22 HTTP 913 GET /apod/ap251002.html
59 10.510196 129.164.179.22 192.168.246.130 HTTP 3984 HTTP/1.1 404 Not Found
61 13.353735 192.168.246.130 129.164.179.22 HTTP 913 GET /apod/ap251002.html
64 13.455577 129.164.179.22 192.168.246.130 TLSv1.2 4013 HTTP/1.1 404 Not Found
66 16.479105 192.168.246.130 129.164.179.22 HTTP 913 GET /apod/ap251002.html
69 16.593095 129.164.179.22 192.168.246.130 HTTP 3984 HTTP/1.1 404 Not Found
71 19.227968 192.168.246.130 129.164.179.22 HTTP 913 GET /apod/ap251002.html
74 19.323129 129.164.179.22 192.168.246.130 HTTP 3984 HTTP/1.1 404 Not Found
76 22.162287 192.168.246.130 129.164.179.22 HTTP 916 GET /apod/lib/edlinks.
80 22.332358 129.164.179.22 192.168.246.130 HTTP 877 HTTP/1.1 200 OK (text
82 22.346492 192.168.246.130 129.164.179.22 HTTP 786 GET /apod/apod.gif HT
Frame 34: Packet, 4007 bytes on wire (32056 bits),
Ethernet II, Src: VMware_e6:d6:48 (00:50:56:e6:d6:
Internet Protocol Version 4, Src: 129.164.179.22,
Transmission Control Protocol, Src Port: 443, Dst
[2 Reassembled TCP Segments (3065 bytes): #33(1589
Transport Layer Security
Transport Layer Security
[2 Reassembled TLS segments (5484 bytes): #34(3036
Hypertext Transfer Protocol
Line-based text data: text/html (146 lines)
Decrypted TLS (2448 bytes)
Reassembled TLS (5484 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 374 · Displayed: 25 (6.7%)
Profile: Default
Wireshark · Preferences
Transport Layer Security
RSA keys list
Edit...
TLS debug file
Browse...
Reassemble TLS records spanning multiple TCP segments
Reassemble TLS Application Data spanning multiple TLS records
Message Authentication Code (MAC), ignore "mac failed"
Try heuristic sub-dissectors first on ports 443
Pre-Shared Key
(Pre)-Master-Secret log filename
/home/kali/wsharkDemo/sslkeys
Browse...
OK
Cancel
Apply

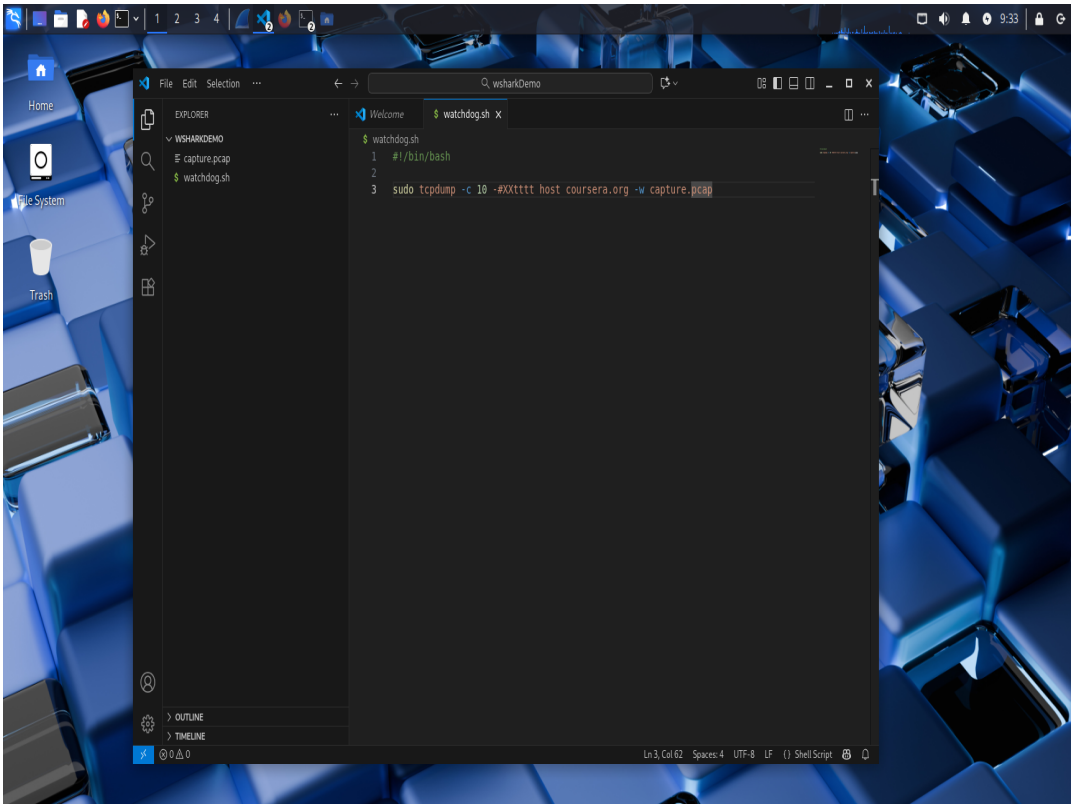

Firefox ESR
Browse the World Wide Web
capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
30 0.359805 192.168.246.130 129.164.179.22 HTTP 855 GET /apod/astropix.html HTTP/1.1
Frame 34: Packet, 4007 bytes on wire (32056 bits), 4007 bytes captured (32056 bits)
Ethernet II, Src: VMware_e6:d6:48 (00:50:56:e6:d6:48), Dst: VMware_1e:c1:dd (00:0c:29:1e:c1
Internet Protocol Version 4, Src: 129.164.179.22, Dst: 192.168.246.130
Transmission Control Protocol, Src Port: 443, Dst Port: 34696, Seq: 1737, Ack: 2672, Len: 3
[2 Reassembled TCP Segments (3065 bytes): #33(1589), #34(1476)]
Transport Layer Security
Transport Layer Security
[2 Reassembled TLS segments (5484 bytes): #34(3036), #34(2448)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Wed, 12 Nov 2025 22:36:10 GMT\r\n
Server: WebServer/1.0\r\n
X-Frame-Options: sameorigin\r\n
Accept-Ranges: bytes\r\n
Content-Length: 5120\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
Strict-Transport-Security: max-age=31536000; includeSubDomains\r\n
Content-Security-Policy: upgrade-insecure-requests\r\n
\r\n
[Request in frame: 30]
[Time since request: 227.271000 milliseconds]
[Request URI: /apod/astropix.html]
[Full request URI: https://apod.nasa.gov/apod/astropix.html]
File Data: 5120 bytes
Line-based text data: text/html (146 lines)
<!doctype html>\n
<html>\n
\n
<head>\n
<b>\n
<i>\n
\n
Due to the lapse in federal government funding, NASA is not updating\n
Packet (4007 bytes)
Reassembled TCP (3065 bytes)
Decrypted TLS (3036 bytes)
Decrypted TLS (2448 bytes)
capture.pcap
Packets: 374 · Displayed: 25 (6.7%)
Profile: Default


capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
30 0.359805 192.168.246.130 129.164.179.22 HTTP 855 GET /apod/astropix.html HTTP/1.1
Frame 34: Packet, 4007 bytes on wire (32056 bits), 4007 bytes captured (32056 bits)
Ethernet II, Src: VMware_e6:d6:48 (00:50:56:e6:d6:48), Dst: VMware_1e:c1:dd (00:0c:29:1e:c1
Internet Protocol Version 4, Src: 129.164.179.22, Dst: 192.168.246.130
Transmission Control Protocol, Src Port: 443, Dst Port: 34696, Seq: 1737, Ack: 2672, Len: 3
[2 Reassembled TCP Segments (3065 bytes): #33(1589), #34(1476)]
Transport Layer Security
Transport Layer Security
[2 Reassembled TLS segments (5484 bytes): #34(3036), #34(2448)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Wed, 12 Nov 2025 22:36:10 GMT\r\n
Server: WebServer/1.0\r\n
X-Frame-Options: sameorigin\r\n
Accept-Ranges: bytes\r\n
Content-Length: 5120\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
Strict-Transport-Security: max-age=31536000; includeSubDomains\r\n
Content-Security-Policy: upgrade-insecure-requests\r\n
\r\n
[Request in frame: 30]
[Time since request: 227.271000 milliseconds]
[Request URI: /apod/astropix.html]
[Full request URI: https://apod.nasa.gov/apod/astropix.html]
File Data: 5120 bytes
Line-based text data: text/html (146 lines)
<!doctype html>\n
<html>\n
\n
<head>\n
<b>\n
<i>\n
\n
Due to the lapse in federal government funding, NASA is not updating\n
Packet (4007 bytes)
Reassembled TCP (3065 bytes)
Decrypted TLS (3036 bytes)
Decrypted TLS (2448 bytes)
capture.pcap
Packets: 374 · Displayed: 25 (6.7%)
Profile: Default


capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.246.130 18.154.84.122 TCP 74 36172 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=717282531 TSecr=0 WS=128
2 0.014091 18.154.84.122 192.168.246.130 TCP 60 443 → 36172 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3 0.014102 192.168.246.130 18.154.84.122 TCP 54 36172 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4 0.016217 192.168.246.130 18.154.84.122 TLSv1.3 2328 Client Hello (SNI=www.coursera.org)
5 0.016398 18.154.84.122 192.168.246.130 TCP 60 443 → 36172 [ACK] Seq=1 Ack=1461 Win=64240 Len=0
6 0.016398 18.154.84.122 192.168.246.130 TCP 60 443 → 36172 [ACK] Seq=1 Ack=2275 Win=64240 Len=0
7 0.025097 18.154.84.122 192.168.246.130 TLSv1.3 1376 Server Hello, Change Cipher Spec, Application Data, Application Data
8 0.025117 192.168.246.130 18.154.84.122 TCP 54 36172 → 443 [ACK] Seq=2275 Ack=1323 Win=65535 Len=0
9 0.025506 192.168.246.130 18.154.84.122 TLSv1.3 118 Change Cipher Spec, Application Data
10 0.025617 18.154.84.122 192.168.246.130 TCP 60 443 → 36172 [ACK] Seq=1323 Ack=2339 Win=64240 Len=0
Frame 9: Packet, 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: VMware_1e:c1:dd (00:0c:29:1e:c1:dd), Dst: VMware_e6:d6:48 (00:50:56:e6:d6:
Internet Protocol Version 4, Src: 192.168.246.130, Dst: 18.154.84.122
Transmission Control Protocol, Src Port: 36172, Dst Port: 443, Seq: 2275, Ack: 1323, Len: 64
Transport Layer Security
[Stream index: 0]
TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.2 (0x0303)
Length: 1
Change Cipher Spec Message
TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Opaque Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 53
Encrypted Application Data: bdf22c6909257507279 87f98d564ff9ea242bc81108f0d517dc55cec8b3
[Application Data Protocol: Hypertext Transfer Protocol]
0000 00 50 56 e6 d6 48 00 0c 29 1e c1 dd 08 00 45 00
0010 00 68 2a 50 40 00 40 06 f2 00 c0 a8 f6 82 12 9a
0020 54 7a 8d 4c 01 bb b2 88 ee 44 0a 4f 18 bb 50 18
0030 ff ff 1e 9a 00 00 14 03 03 00 01 01 17 03 03 00
0040 35 bd f2 2c 69 09 25 75 07 27 98 7f 98 d5 64 ff
0050 9e a2 42 bc 81 10 8f 0d 51 7d c5 5c ec 8b 33 66
0060 64 dc 79 b0 15 54 f0 cc cc 50 a0 5c c6 63 a2 b3
0070 66 9f 44 90 da 93
Payload is encrypted application data (tls.app_data), 53 bytes
Packets: 10
Profile: Default


capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.246.130 18.154.84.122 TCP 74 36172 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=717282531 TSecr=0 WS=128
2 0.014091 18.154.84.122 192.168.246.130 TCP 60 443 → 36172 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3 0.014102 192.168.246.130 18.154.84.122 TCP 54 36172 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4 0.016217 192.168.246.130 18.154.84.122 TLSv1.3 2328 Client Hello (SNI=www.coursera.org)
5 0.016398 18.154.84.122 192.168.246.130 TCP 60 443 → 36172 [ACK] Seq=1 Ack=1461 Win=64240 Len=0
6 0.016398 18.154.84.122 192.168.246.130 TCP 60 443 → 36172 [ACK] Seq=1 Ack=2275 Win=64240 Len=0
7 0.025097 18.154.84.122 192.168.246.130 TLSv1.3 1376 Server Hello, Change Cipher Spec, Application Data, Application Data
8 0.025117 192.168.246.130 18.154.84.122 TCP 54 36172 → 443 [ACK] Seq=2275 Ack=1323 Win=65535 Len=0
9 0.025506 192.168.246.130 18.154.84.122 TLSv1.3 118 Change Cipher Spec, Application Data
10 0.025617 18.154.84.122 192.168.246.130 TCP 60 443 → 36172 [ACK] Seq=1323 Ack=2339 Win=64240 Len=0
Frame 4: Packet, 2328 bytes on wire (18624 bits), 2328 bytes captured (18624 bits)
Ethernet II, Src: VMware_1e:c1:dd (00:0c:29:1e:c1:dd), Dst: VMware_e6:d6:48 (00:50:56:e6:d6:
Internet Protocol Version 4, Src: 192.168.246.130, Dst: 18.154.84.122
Transmission Control Protocol, Src Port: 36172, Dst Port: 443, Seq: 1, Ack: 1, Len: 2274
Transport Layer Security
0000 00 50 56 e6 d6 48 00 0c 29 1e c1 dd 08 00 45 00
0010 09 0a 2a 4d 40 00 40 06 e9 61 c0 a8 f6 82 12 9a
0020 54 7a 8d 4c 01 bb b2 88 e5 62 0a 4f 13 91 50 18
0030 fa f0 27 3c 00 00 16 03 01 08 dd 01 00 08 d9 03
0040 03 38 50 54 f1 b5 84 c3 47 66 0a dd f3 80 5c 63
0050 bc 3b af 06 f5 f8 f2 98 16 4f cd bf 35 72 ca ed
0060 62 20 92 e2 36 27 dc 60 23 6a d0 da b7 aa 2a 86
0070 e9 a5 e0 8f 95 8a 82 74 0c 22 71 3e fd 32 a4 6e
0080 5b bd 00 22 13 01 13 03 13 02 c0 2b c0 2f cc a9
0090 cc a8 c0 2c c0 30 c0 0a c0 09 c0 13 c0 14 00 9c
00a0 00 9d 00 2f 00 35 01 00 08 6e 00 00 00 15 00 13
00b0 00 00 10 77 77 77 2e 63 6f 75 72 73 65 72 61 2e
00c0 6f 72 67 00 17 00 00 ff 01 00 01 00 00 0a 00 10
00d0 00 0e 11 ec 00 1d 00 17 00 18 00 19 01 00 01 01
00e0 00 0b 00 02 01 00 00 10 00 0e 00 0c 02 68 32 08
00f0 68 74 74 70 2f 31 2e 31 00 05 00 05 01 00 00 00
0100 00 00 22 00 0a 00 08 04 03 05 03 06 03 02 03 00
0110 12 00 00 00 33 05 2f 05 2d 11 ec 04 c0 54 25 7a
0120 22 49 9d 28 1c ad 45 6b 87 ba da 90 7e 62 9b a4
0130 c7 11 09 06 4f 74 e6 38 96 81 4e 6c 40 3b c5 a1
0140 00 fc 0c 50 ae 98 23 34 f1 2a 6d ab 7c 35 c6 66
capture.pcap
Packets: 10
Profile: Default


File Edit Selection
wsharkDemo
EXPLORER
WSHARKDEMO
capture.pcap
watchdog.sh
Session Actions Edit View Help
kali@kali: ~/wsharkDemo
0×0030: ffff 1e5a 0000 ... Z ..
10 packets captured
25 packets received by filter
0 packets dropped by kernel
(kali㉿kali)-[~/wsharkDemo]
$ sudo chmod +w watchdog.sh
$ ls -l
total 4
-rwxrwxr-x 1 kali kali 58 Nov 12 09:17 watchdog.sh
$ sudo chmod o+w watchdog.sh
$ ls -l
total 4
-rwxrwxrwx 1 kali kali 58 Nov 12 09:17 watchdog.sh
$ ./watchdog.sh
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10 packets captured
22 packets received by filter
0 packets dropped by kernel
$ ls
capture.pcap watchdog.sh
$ tcpdump -r capture.pcap
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot length 26
OUTLINE
TIMELINE
Ln 3, Col 62 Spaces: 4 UTF-8 LF {} Shell Script


File Edit Selection
wsharkDemo
EXPLORER
WSHARKDEMO
capture.pcap
watchdog.sh
Welcome
watchdog.sh
1 #!/bin/bash
2
3 sudo tcpdump -c 10 -#XXtttt host coursera.org -w capture.pcap
OUTLINE
TIMELINE
Ln 3, Col 62 Spaces: 4 UTF-8 LF {} Shell Script