Comprehensive Nikto Report — Extracted from Screen Recording

Video source: Screen Recording 2025-09-14 205010.mp4

Objective

Run Nikto web vulnerability scan and analyze results captured in the provided screen recording.

Method

Extracted representative frames from the recording at 5-second intervals and reviewed the terminal output visible in those frames to compile findings.

Findings (interpreted from the video frames)

- The Nikto command executed: nikto -h http://93.184.216.34 --host example.com targeting port 80 (HTTP).
- The output confirms multiple IP addresses resolved for the hostname, indicating CDN/load balancing.
- No server banner was retrieved (server type/version hidden).
- Missing security headers detected: X-Frame-Options and X-Content-Type-Options.
- Timestamp observed in video: 2025-09-14 around 21:33:10 (GMT+5.5).
- The video also shows navigation commands (e.g., `cd nikto`) prior to running the scan.

Detailed Analysis

1. Multiple IPs & Infrastructure: The presence of multiple IPv4 and IPv6 addresses suggests the target uses a distributed infrastructure (CDN or load balancer). This affects vulnerability scanning as responses may vary across endpoints.

2. Missing Security Headers: The lack of X-Frame-Options allows clickjacking risks; adding X-Frame-Options: SAMEORIGIN mitigates this. The missing X-Content-Type-Options: nosniff may allow MIME-sniffing related attacks; add the header to prevent browsers from guessing content types.

3. Banner Hiding: No banner reduces fingerprinting; however, maintain patching and hardening practices regardless.

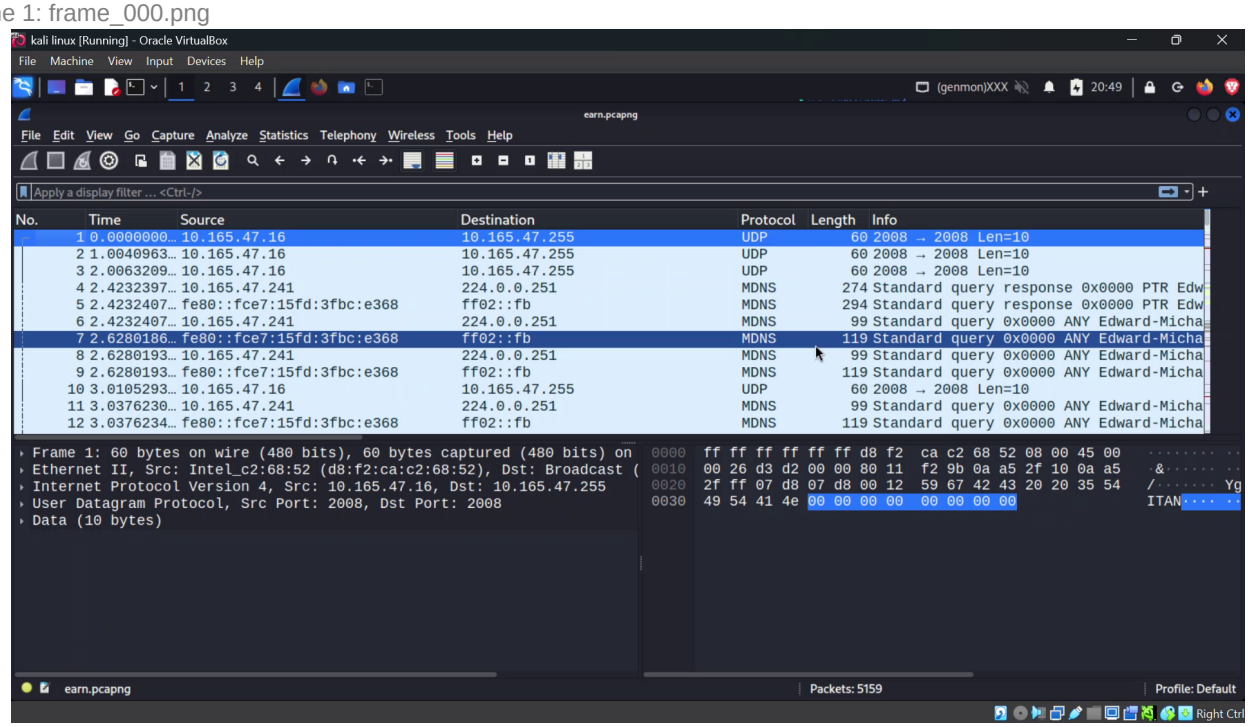
Recommendations (detailed)

- Add security headers at the webserver or application level:
• For Apache (example):
`Header always set X-Frame-Options "SAMEORIGIN"`
`Header set X-Content-Type-Options "nosniff"`
• For Nginx (example):
`add_header X-Frame-Options "SAMEORIGIN";`
`add_header X-Content-Type-Options "nosniff";`

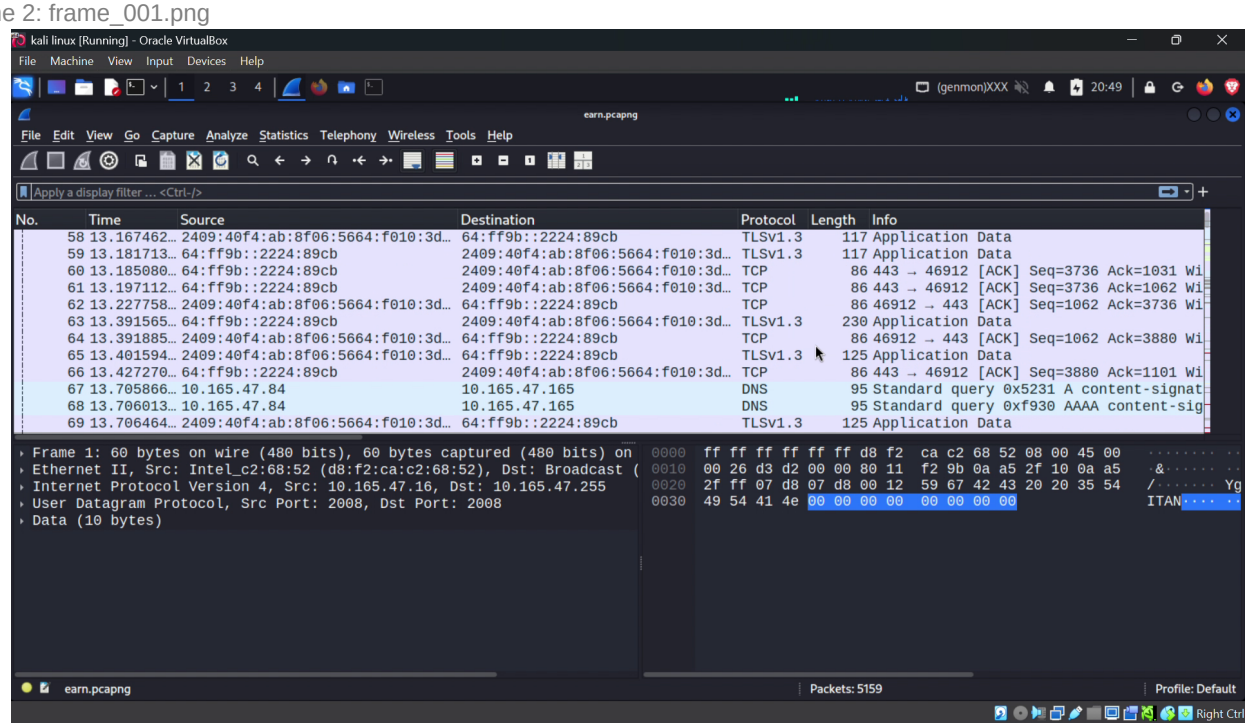
- Enforce HTTPS and redirect HTTP to HTTPS. Use HSTS (Strict-Transport-Security) header.
- Implement Content Security Policy to restrict sources for scripts and frames.
- Schedule automated scans and include multiple scan points to capture CDN variability.
- Keep server software and modules updated; maintain a vulnerability remediation workflow.
- If required, perform authenticated scans to find issues in authenticated areas.

Appendix: Extracted Frames from Recording

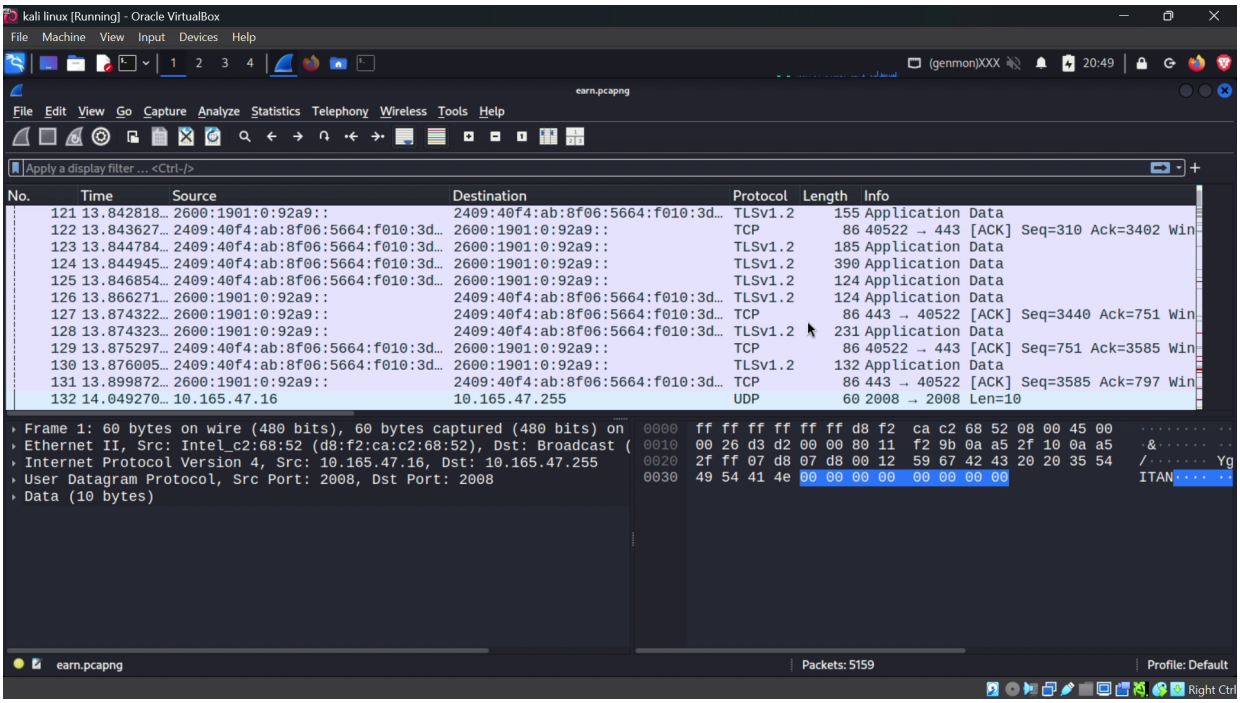
Frame 1: frame_000.png



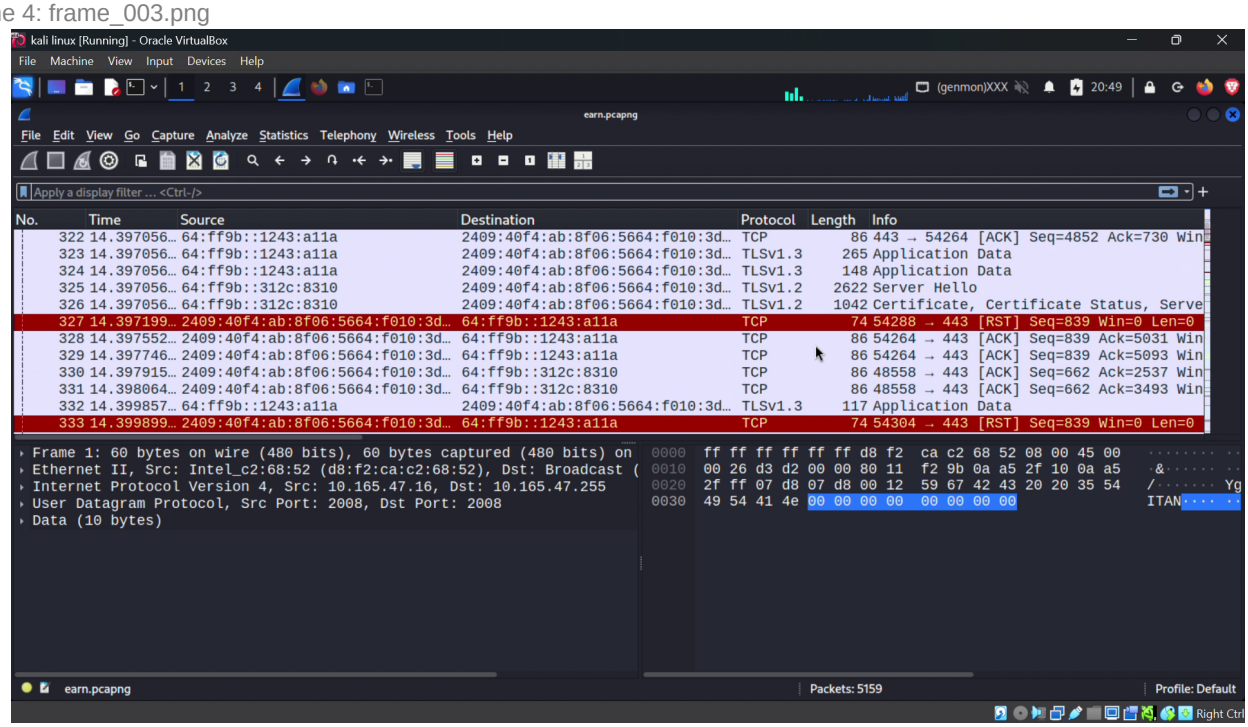
Frame 2: frame_001.png



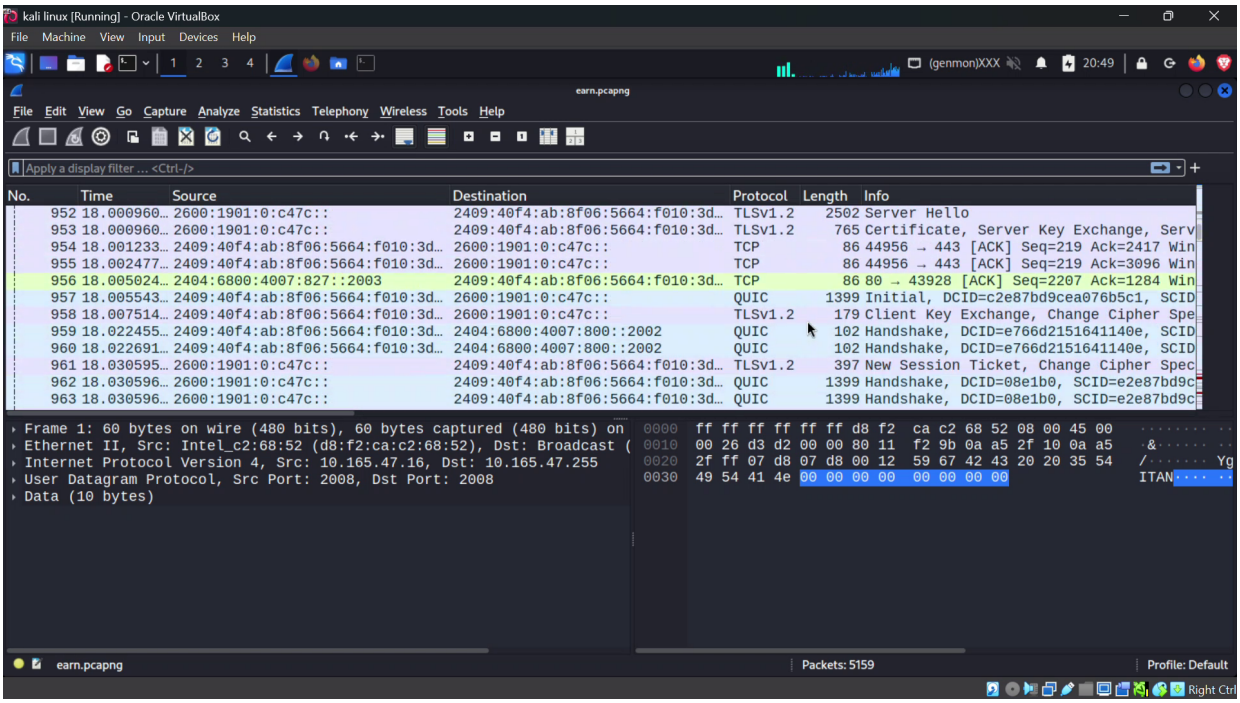
Frame 3: frame_002.png



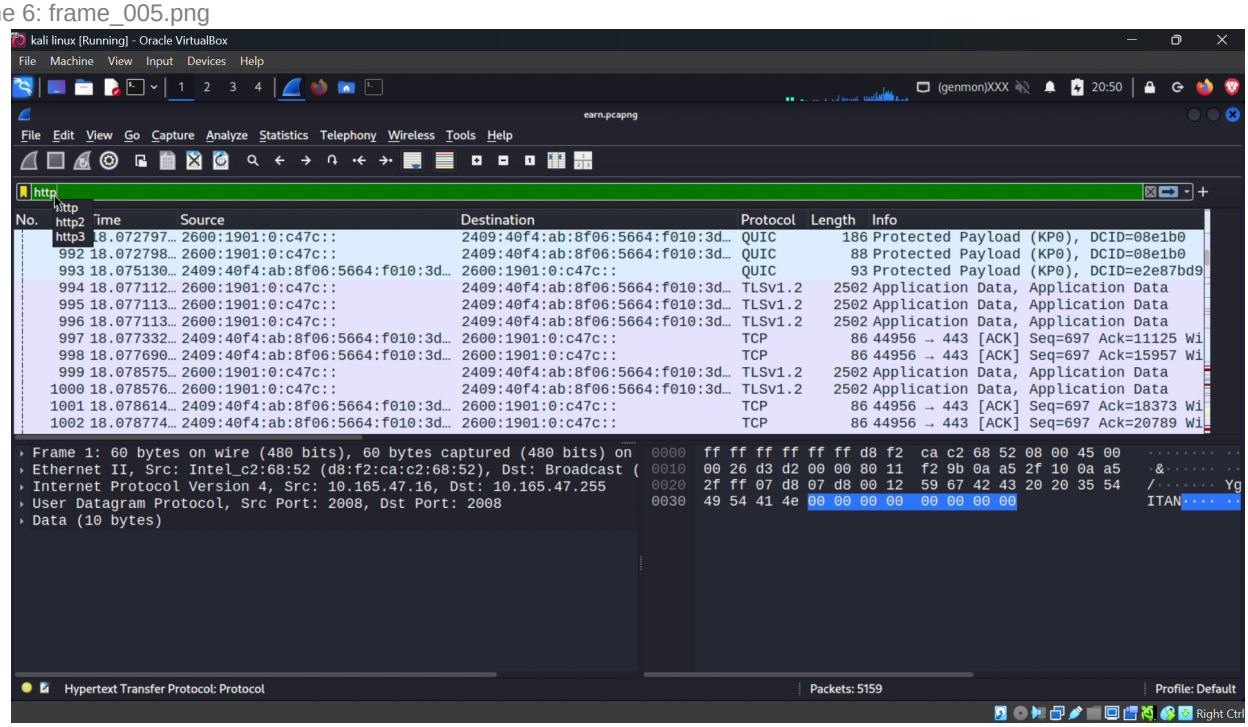
Frame 4: frame_003.png



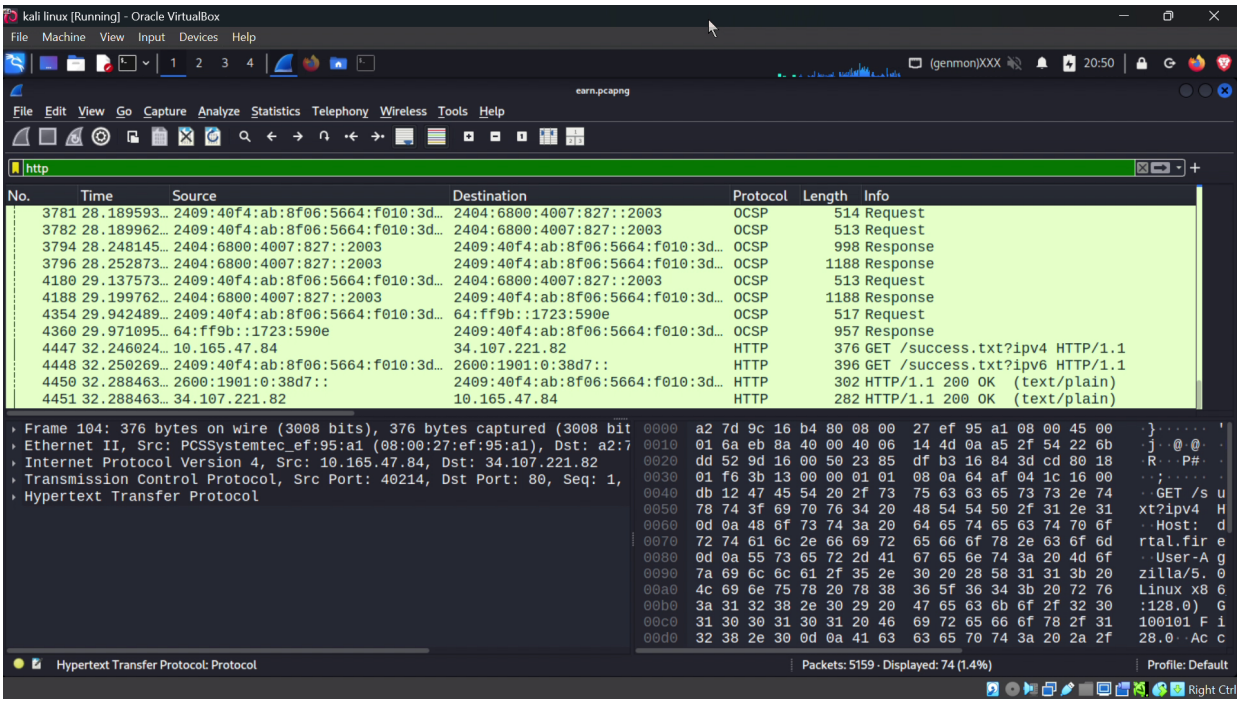
Frame 5: frame_004.png



Frame 6: frame_005.png



Frame 7: frame_006.png


kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(genmon)XXX 20:50
earn.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
3781 28.189593… 2409:40f4:ab:8f06:5664:f010:3d… 2404:6800:4007:827::2003 OCSP 514 Request
3782 28.189962… 2409:40f4:ab:8f06:5664:f010:3d… 2404:6800:4007:827::2003 OCSP 513 Request
3794 28.248145… 2404:6800:4007:827::2003 2409:40f4:ab:8f06:5664:f010:3d… OCSP 998 Response
3796 28.252873… 2404:6800:4007:827::2003 2409:40f4:ab:8f06:5664:f010:3d… OCSP 1188 Response
4180 29.137573… 2409:40f4:ab:8f06:5664:f010:3d… 2404:6800:4007:827::2003 OCSP 513 Request
4188 29.199762… 2404:6800:4007:827::2003 2409:40f4:ab:8f06:5664:f010:3d… OCSP 1188 Response
4354 29.942489… 2409:40f4:ab:8f06:5664:f010:3d… 64:ff9b::1723:590e OCSP 517 Request
4360 29.971095… 64:ff9b::1723:590e 2409:40f4:ab:8f06:5664:f010:3d… OCSP 957 Response
4447 32.246024… 10.165.47.84 34.107.221.82 HTTP 376 GET /success.txt?ipv4 HTTP/1.1
4448 32.250269… 2409:40f4:ab:8f06:5664:f010:3d… 2600:1901:0:38d7:: HTTP 396 GET /success.txt?ipv6 HTTP/1.1
4450 32.288463… 2600:1901:0:38d7:: 2409:40f4:ab:8f06:5664:f010:3d… HTTP 302 HTTP/1.1 200 OK (text/plain)
4451 32.288463… 34.107.221.82 10.165.47.84 HTTP 282 HTTP/1.1 200 OK (text/plain)
Frame 104: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bit
Ethernet II, Src: PCSSystemtec_ef:95:a1 (08:00:27:ef:95:a1), Dst: a2:7
Internet Protocol Version 4, Src: 10.165.47.84, Dst: 34.107.221.82
Transmission Control Protocol, Src Port: 40214, Dst Port: 80, Seq: 1,
Hypertext Transfer Protocol
0000 a2 7d 9c 16 b4 80 08 00 27 ef 95 a1 08 00 45 00
0010 01 6a eb 8a 40 00 40 06 14 4d 0a a5 2f 54 22 6b
0020 dd 52 9d 16 00 50 23 85 df b3 16 84 3d cd 80 18
0030 01 f6 3b 13 00 00 01 01 08 0a 64 af 04 1c 16 00
0040 db 12 47 45 54 20 2f 73 75 63 63 65 73 73 2e 74
0050 78 74 3f 69 70 76 34 20 48 54 54 50 2f 31 2e 31
0060 0d 0a 48 6f 73 74 3a 20 64 65 74 65 63 74 70 6f
0070 72 74 61 6c 2e 66 69 72 65 66 6f 78 2e 63 6f 6d
0080 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f
0090 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20
00a0 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 72 76
00b0 3a 31 32 38 2e 30 29 20 47 65 63 6b 6f 2f 32 30
00c0 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31
00d0 32 38 2e 30 0d 0a 41 63 63 65 70 74 3a 20 2a 2f
Hypertext Transfer Protocol: Protocol
Packets: 5159 · Displayed: 74 (1.4%)
Profile: Default
Right Ctrl