COMP2322 Computer Networking

Lab1 Report: Wireshark

Author
Wang Yuqi
[redacted]

Lecturer
Dr. LOU Wei

BsC in Computer Science
Academic year: 2024/2025 Sem 2

Questions

Q0: Trace File

Answer:

The trace file for this lab report is attached as `lab1_tracefile.pcapng`.

Disclaimer To protect my **personal privacy**, only a selected subset of the original trace file is included. This partial trace retains lab-relevant traffic while scrubbing other sensitive data.

Sensitive Info The full trace contained these info that I do not wish to disclose:

- Public IPs of my private GPU compute nodes
- Public IPs of my private VPN network
- TLS handshake and key exchange messages
- Network activity that reveals my software usage and browsing habits

Q1: List 3 Protocols

Answer:

- TCP (*Transmission Control Protocol*)
- ICMP (*Internet Control Message Protocol*)
- TLSv1.2 (*Transport Layer Security*)

Q2: HTTP Time Elapsed

Time	Source	Destination	Protocol	Len	Info
6.953364	172.20.10.10	128.119.245.12	HTTP	466	GET HTTP/1.1
7.259930	128.119.245.12	172.20.10.10	HTTP	492	HTTP/1.1 200 OK

Alternatively, in ***Time-of-day* format**:

Time	Source	Destination	Protocol	Len	Info
13:19:13.765428	172.20.10.10	128.119.245.12	HTTP	466	GET HTTP/1.1
13:19:14.071994	128.119.245.12	172.20.10.10	HTTP	492	HTTP/1.1 200 OK

Answer:

Default format:	7.259930 - 6.953364 = 0.306566
Time-of-day format:	13:19:14.071994 - 13:19:13.765428 ≈ 00:00:00.307

Q3: Internet Address

Based on the results from Q2, my computer address is the private address 172.20.10.10. Whereas, the internet address of gaia.cs.umass.edu is 128.119.245.12.

Double checking with My Trace Route:

```
My traceroute  [v0.95]
[redacted] (172.20.10.10) ->
gaia.cs.umass.edu (128.119.245.12)
```

Answer:

	IP Address	Domain Name
My Computer	172.20.10.10 (private)	[redacted]
UMass Website	128.119.245.12 (public)	gaia.cs.umass.edu

(See Next Page)

Q4: Print HTTP Messages (HTTP expanded, everything else collapsed as required)

Answer:

HTTP GET

```
      Time             Source          Destination       Protocol Length Info
1663  13:19:13.765428  172.20.10.10    128.119.245.12    HTTP     466    GET /wireshark-labs/INTRO-
wireshark-file1.html HTTP/1.1

Frame 1663: 466 bytes on wire (3728 bits), 466 bytes captured (3728 bits) on interface en0, id 0
Ethernet II, Src: [redacted], Dst: [redacted]
Internet Protocol Version 4, Src: 172.20.10.10, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49418, Dst Port: 80, Seq: 1, Ack: 1, Len: 412

Hypertext Transfer Protocol:
  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Request Method: GET
    Request URI: /wireshark-labs/INTRO-wireshark-file1.html
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  User-Agent: [redacted]
  Accept-Language: [redacted]
  Accept-Encoding: [redacted]
  DNT: 1\r\n
  Sec-GPC: 1\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Priority: u=0, i\r\n
  \r\n
  [Response in frame: 1715]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

HTTP OK

```
      Time             Source          Destination       Protocol Length Info
1715  13:19:14.071994  128.119.245.12  172.20.10.10      HTTP     492    HTTP/1.1 200 OK (text/html)

Frame 1715: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface en0, id 0
Ethernet II, Src: [redacted], Dst: [redacted]
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.10
Transmission Control Protocol, Src Port: 80, Dst Port: 49418, Seq: 1, Ack: 413, Len: 438

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: Sun, 26 Jan 2025 05:19:14 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Sat, 25 Jan 2025 06:59:01 GMT\r\n
  ETag: "51-62c8260cc60b2"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 81\r\n
    [Content length: 81]
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [Request in frame: 1663]
  [Time since request: 0.306566000 seconds]
  [Request URI: /wireshark-labs/INTRO-wireshark-file1.html]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
  File Data: 81 bytes
  Line-based text data: text/html (3 lines)
```