Question A

1)web browser ของผู้เรียนส่ง HTTP request ไปยัง gaia.cs.umass.edu โดยใช้ HTTP version ใด? และ web server ตอบกลับโดยใช้ HTTP version ใด?

Answer ทั้งที่ web browser request และ web server ตอบกลับใช้ http version HTTP/1.1 (จาก protocol http header line)

2)ใน HTTP request ที่ส่งไป ฝั่ง web browser บอกหรือระบุให้ฝั่งweb server รู้ว่ารองรับภาษาใดบ้าง?

Answer ภาษาไทย,ภาษาอังกฤษ และภาษาอาร์มีเนีย (จาก protocol http field Accept-Language)

3)IP address ของเครื่องคอมพิวเตอร์ของผู้เรียนและของเครื่อง gaia.cs.umass.edu คือหมายเลขใด?

Answer ip address ของเครื่องผู้เรียนคือ 10.66.9.225 และของเครื่อง gain.cs.umass.edu คือ 128.119.245.12 (จาก internet protocol field source address,destination address)

4)ใน HTTP response มีการส่ง status code และ response phrase ใด มายังweb browser?

Answer ส่ง status code มาคือ 200 และ response pharse คือ OK (จาก protocol http field status code และ response phrase)

5)ไฟล์ HTML ที่ได้รับจาก web server ระบุไว้ว่าถูกแก้ไขล่าสุดเมื่อเวลาใด?

Answer Mon, 18 Dec 2023 06:59:01 GMT

6)ขนาดของ HTML content ที่ส่งจาก web server มายัง browser มีขนาดกี่ bytes?

Answer 128 bytes

7)ใน HTTP header ของ HTTP response ระบุค่าContent-Type เป็นค่าอะไร? ค่าดังกล่าวมีความหมายอย่างไร?

Answer content type คือ text/html; charset=UTF-8\r\n

text/html บ่งบอกว่า เป็นสื่อทาง internet ที่ใช้ html

charset = UTF-8 บ่งบอกว่า ใช้การเข้ารหัสตัวอักษรด้วยวิธี UTF-8

Question B

8)ตรวจสอบHTTP header ของHTTP GET request แรกซึ่งส่งจาก web browser ไปยัง web server พบว่ามีบรรทัด “IF-MODIFIED-SINCE”หรือไม่?

Answer ไม่พบ

9)ตรวจสอบHTTP header ของHTTP response แรกพบว่า web server ส่งเนื้อหาไฟล์มาพร้อมในHTTPresponse ด้วยหรือไม่?ผู้เรียนสามารถระบุได้จากอะไร?

Answer ส่งมาพร้อมโดยระบุจาก content-Type คือ text/html ซึ่งมีความหมายว่ามีการรับไฟล์ htmlกัน

10)ตรวจสอบHTTP header ของHTTP response แรก พบว่า web server ส่ง ETag มาด้วยค่าดังกล่าวมีค่าเป็นอะไร?

Answer "173-60cc348ec54af" (จาก protocol http field Etag)

11)ตรวจสอบ HTTP header ของ HTTP GET request ที่สอง ซึ่งส่งจาก web browser ไปยัง web server พบว่ามีบรรทัดที่ระบุค่า ETag ส่งไปให้ serverด้วยหรือไม่? ถ้าส่งไปด้วยค่าดังกล่าวอยู่ใน field ชื่อว่าอะไร?

Answer มี ค่าดังกล่าวอยู่ใน field If-None-Match (จาก protocol http)

12)ตรวจสอบHTTP header ของHTTP GET request ที่สอง ซึ่งส่งจาก web browser ไปยัง web server พบว่ามีบรรทัด "IF-MODIFIED-SINCE"หรือไม่?ถ้ามีค่าของfield ดังกล่าวเป็นค่าอะไร?

Answer มี ค่าของ field นั้นคือ If-Modified-Since: Mon, 18 Dec 2023 06:59:01 GMT

13)ตรวจสอบHTTP header ของ HTTP response ที่สองซึ่งweb server ส่งตอบ HTTP GET request ที่สองพบว่ามีHTTPstatus code และ response phraseเป็นอะไร? พบว่า web server ส่งเนื้อหาไฟล์มาพร้อมในHTTPresponse ด้วยหรือไม่? จงอธิบาย

Answer HTTPstatus code คือ 304 , response phrase คือ Not Modified และไม่มีการส่งไฟล์มาพร้อม HTTP response หมายความว่า เครื่องได้ทำการ request content ที่ไม่ได้มีการ update ตั้งแต่ครั้งล่าสุดที่เราได้ access ดังนั้น web browser จะทำการบันทึก cache เพื่อที่เราจะไม่ต้อง download ข้อมูลเดิม

14)ค้นคว้าข้อมูลเพิ่มเติมจากอินเทอร์เน็ต และเขียนอธิบายว่าค่า ETag มีเอาไว้เพื่อจุดประสงค์อะไร?

Answer Etag คือ field ใน HTTP response header ที่ทำงานร่วมกับการ caching โดยจะเช็คได้ว่า resource มีการเปลี่ยนแปลงหรือไม่ เพื่อจะไม่จำเป็นต้อง re-download ซ้ำ

15)สามารถกรองให้ Packet List Pane แสดงแค่ HTTP request โดยใช้ http.request เป็น Display filter ถ้าหากต้องการกรองให้แสดงเฉพาะ HTTP responseจะต้องใช้ Display filter ว่าอะไร?

Answer http.response

Question C

16)web browserส่งHTTP GET request ออกไปกี่ message? packet หมายเลขใดในไฟล์traceที่เป็น GET message เพื่อร้องขอเอกสาร USBill of Rights?

Answer web browser ส่ง HTTP GET request ออกไป 1 message เป็น packet หมายเลข 66ใน trace file

17)packet หมายเลขใดที่มี status code และ response phrase เพื่อตอบ HTTP GET request ในข้อ 16)?

Answer packet หมายเลข 70 (จาก packet list pane column No.)

18)จากHTTP responseในข้อ17)พบว่ามี statuscode และ response phraseเป็นอะไร?

Answer statuscode คือ 200 และ response phrase คือ OK (จาก protocol http field status code และ response code)

19)จากHTTP responseในข้อ 17)พบว่า Content-Length มีค่าเป็นเท่าไร?

Answer มีค่า Content-Length คือ 4500 bytes (จาก protocol http field Content-Length)

20)ต้องใช้ TCP segments กี่ segment เพื่อนำส่ง HTTP response และเอกสารUS Bill of Rights?

Answer 3 segments (นับจาก Packet List Pane)

21)หากต้องการให้ Packet List Pane แสดงเฉพาะทุกpacketsตามข้อ 20)จะต้องใช้ Display filter ใด?

Answer http.file_data

22)หากต้องการให้ Wireshark คำนวณขนาด packet เฉลี่ยจาก packets ทั้งหมดในข้อ 21)ต้องทำอย่างไรบ้าง? จงอธิบายวิธีการ

Answer ไปที่ Statistics>>Packet Lengths>>และ filter ว่า http.file_data

23)จากข้อ 21)แต่ละ packet นำส่งData จากเอกสาร US Bill of Rights เป็นขนาดกี่ bytes สามารถหาขนาดของข้อมูลที่นำส่งได้จากไหนใน Wireshark? จงอธิบาย

Answer แต่ละ packet มีขนาดเป็น 1380,1380 และ 721 bytes ตามลำดับ โดยสามารถดูได้ที่ field ชื่อ file Data

24)จากคำตอบของข้อ 23)มีการระบุตัวเลขใน header หรือไม่ ว่าแต่ละ packet นำส่ง Data ขนาดกี่ bytes?

Answer ไม่มี

Question D

25)web browserส่ง HTTP GET request ออกไปกี่ message?แต่ละ GET request ถูกส่งไปยัง Internet Address ใดบ้าง?

โดย object ที่ทำการ request ขอได้มาจาก head line ใน protocol http ส่วน internet address ได้มาจาก field source address,destination address ใน internet protocol

Answer มี 5 message โดย

Message แรกเป็นการ request ขอ HTTP-wireshark-file4.html ที่ internet address 128.119.245.12

Message สองเป็นการ request ขอ pearson.png ที่ internet address 128.119.245.12

Message สามเป็นการ request ขอ 8E_cover_small.jpg ที่ internet address 178.79.137.164

Message สี่เป็นการ request ขอ favicon.ico ที่ internet address 128.119.245.12

Message ห้าเป็นการ request ขอ contenttest.txt ที่ internet address 103.21.25.201

26)หากพิจารณาเฉพาะ HTTP response ที่ส่งไฟล์ HTTP-wireshark-file4.html มายัง web browser ผู้เรียนสามารถบอกได้หรือไม่ว่ามีไฟล์ภาพชื่ออะไรบ้างที่ถูกฝังหรืออ้างอิงถึงใน web page?จงอธิบาย

Answer สามารถบอกได้จาก field Line-based text data ตรงส่วน img src ซึ่งมี 8E_cover_small.jpg และ pearson.png

27)ใน HTTP response ที่ส่งไฟล์ภาพตามข้อ 26)มายังweb browserระบุContent-Type ไว้เป็นอะไรบ้าง?

Answer HTTP response ของภาพ 8E_cover_small.jpg มี Content-Length เป็น 0 byte

ส่วน HTTP response ของภาพ peason.png มี Content-Length เป็น 3267 bytes

28)ผู้เรียนสามารถบอกได้หรือไม่ว่า web browser ทำการดาวน์โหลดแบบไฟล์ภาพ 2 สอง แบบทีละภาพ หรือมีช่วงเวลาที่ดาวน์โหลดทั้งสองภาพไปพร้อมๆ กัน(parallel)? จงอธิบาย?

Answer มีการโหลดแบบทีละภาพ เพราะว่า ภาพที่2ถูก request หลังจากที่มีการ response ภาพแรกมาแล้ว

โดยคำตอบได้มาจากการพิจารณา time relative จาก column time

29)หลังจากได้รับ HTTP GET message แรกจาก web browser แล้ว web server ตอบกลับด้วย status code และ response phrase ใด?

Answer Status Code : 401, Response Phrase : Unauthorized (สังเกตจาก Packet Details Pane ใน protocol http field ชื่อ Status Code, Response Phrase)

30)เทียบกับการทดลองก่อนหน้านี้ มี field ใดเพิ่มเติมใน HTTP headerของHTTP response ตามข้อ29)?

Answer มี field ชื่อ WWW-Authenticate (จาก packet detail pane ใน protocol http)

31)เมื่อweb browser ของผู้เรียนส่ง HTTP GET message ออกไปเป็นครั้งที่ 2 มี field ใดปรากฏเพิ่มเติมเมื่อเทียบกับ HTTP GET message อันแรก

Answer มี field Authorizetion (จาก packet detail pane ใน protocol http)