**ĐỒ ÁN WIRESHARK  
BẮT VÀ PHÂN TÍCH GÓI TIN**

**QUY ĐỊNH:**

* Đồ án làm cá nhân
* **X** là 2 chữ số cuối của MSSV. Ví dụ MSSV là 1812123 thì **X**=23
* Các bài làm giống nhau bất kể vì lý do gì đều bị 0 điểm phần thực hành.
* **Bài nộp MSSV.zip gồm:**
* 1**.** File **MSSV.docx/pdf** trả lời các câu hỏi và bắt buộc phải có hình chụp chứng minh (cần đóng khung, chú thích các thông tin quan trọng của hình chụp) ứng với từng câu trả lời. Khi chụp hình phải chụp đầy đủ và có 1 phần Desktop Background.
* 2. File gói tin Wireshark **ICMP\_MSSV.pcapng, HTTP\_MSSV.pcapng và FTP\_MSSV.pcapng**
* Lưu ý: Sinh viên chỉ trình bày phần phân tích gói tin, không trình bày phần cấu hình các dịch vụ vào báo cáo.

**ĐỀ BÀI**

**Bài 1: ICMP**

1. Thiết lập card mạng máy ảo là Host-Only.
2. Cấu hình IP để máy thật và máy ảo có thể ping nhau:
   1. Card VMnet 1 trên máy thật:

* IP: 192.168.X.2
* Subnet mask: 255.255.255.0
  1. Máy ảo: 192.168.X.1
* IP: 192.168.X.1
* Subnet mask: 255.255.255.0

1. Bắt gói tin ICMP giữa máy thật và máy ảo (lưu file với tên **ICMP\_MSSV.pcapng)**, trả lời các câu hỏi:
   1. Mục đích của việc ping?
   2. Có bao nhiêu các gói tin trong quá trình ping?
   3. Địa chỉ MAC nguồn? MAC đích?
   4. Địa chỉ IP nguồn? IP đích?
   5. Nội dung phần Data của gói tin ICMP?

**Bài 2: HTTP**

1. Thực hiện các bước sau:
2. Start Wireshark
3. Mở Chrome
4. Truy cập: gaia.cs.umass.edu
5. Bấm vào 1 link bất kỳ trong web.
6. Truy cập lần 1: gaia.cs.umass.edu/ethereal-labs/lab2-1.html
7. Truy cập lần 2: gaia.cs.umass.edu/ethereal-labs/lab2-1.html
8. Truy cập: gaia.cs.umass.edu/ethereal-labs/lab2-3.html
9. Stop Wireshark
10. Lưu file với tên **HTTP\_MSSV.pcapng**
11. Phân tích gói tin vừa bắt được và trả lời các câu hỏi sau:
12. Trình duyệt của bạn chạy HTTP phiên bản 1.0 hay 1.1? Phiên bản của HTTP được server chạy là bao nhiêu?
13. Ngôn ngữ mà trình duyệt web của bạn chỉ ra nó có thể chấp nhận server?
14. Địa chỉ IP của máy bạn và gaia.cs.umass.edu server?
15. Mã trả về từ server cho trình duyệt của bạn và ý nghĩa của nó?
16. Thời điểm file HTML mà bạn đang nhận được chỉnh sửa lần cuối ở server?
17. Có bao nhiêu byte trong nội dung được trả về cho trình duyệt của bạn?
18. Kiểm tra nội dung của yêu cầu HTTP GET đầu tiên từ trình duyệt của bạn tới server. Bạn có thấy 1 dòng “IF-MODIFIED-SINCE” trong HTTP GET?
19. Kiểm tra các nội dung phản hồi của server. Server có trả về nội dung của file một cách rõ ràng không?
20. Tiếp theo kiểm tra các nội dung của yêu cầu HTTP GET thứ hai từ trình duyệt của bạn tới server. Bạn có thấy dòng “IF-MODIFIED-SINCE” trong HTTP GET? Nếu có thì đó là thông tin gì sau “IF-MODIFIED-SINCE:” header? Cho biết ý nghĩa của nó?
21. Cho biết mã trả về từ server cho HTTP GET thứ hai? Server có trả về rõ ràng nội dung của các file? Giải thích tại sao lại như vậy?

**Bài 3: FTP**

1. Thiết lập card mạng máy ảo là Host-Only.
2. Cấu hình IP để máy thật và máy ảo có thể ping nhau:
3. Card VMnet 1 trên máy thật:
   * IP: 192.168.X.2
   * Subnet mask: 255.255.255.0
4. Máy ảo: 192.168.X.1
   * IP: 192.168.X.1
   * Subnet mask: 255.255.255.0
5. Cài đặt và cấu hình FTP Server trên máy ảo, FTP Client trên máy thật.

FTP Server: <https://filezilla-project.org/download.php?type=server>

FTP Client: <https://filezilla-project.org/download.php?type=client>

1. Thực hiện các bước sau:
2. Start Wireshark ở máy thật
3. FTP Client kết nối đến FTP Server với user/password là **họ tên/MSSV** (Sinh viên cấu hình ở câu 3 ở trên)
4. FTP Client download 1 file bất kỳ từ FTP Server.
5. FTP Client upload 1 file bất kỳ lên FTP Server
6. FTP Client xóa 1 file bất kỳ trên FTP Server
7. Stop Wireshark
8. Lưu file với tên **FTP\_MSSV.pcapng**
9. Phân tích các gói tin và trả lời các câu hỏi:
10. Có bao nhiêu loại gói tin FTP? Giải thích ý nghĩa từng gói?
11. IP nguồn, IP đích của các gói tin FTP?
12. MAC nguồn, MAC đích của các gói tin FTP?
13. FTP sử dụng port ở server và client là bao nhiêu?
14. FTP đang sử dụng mode passive hay active?
15. Chúng ta có lấy được thông tin user và password từ các gói tin FTP không?