

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOAN AN TOÀN THÔNG TIN**

---



**BÁO CÁO THỰC HÀNH**

**Bài 8: Bắt dữ liệu mạng**

**Họ và tên: Vũ Thành Long**

**Mã sinh viên: B21DCAT012**

**Nhóm: 06**

**Môn học: Thực tập cơ sở**

**Giảng viên giảng dạy: Nguyễn Hoa Cường**

**Hà Nội, 2024**

# Mục lục

I. Tìm hiểu lý thuyết: .....	2
– tcpdump: .....	2
– Wireshark: .....	2
– NetworkMiner: .....	3
II. Mô tả cài đặt & kết quả: .....	3
– Sử dụng tcpdump: .....	3
– Sử dụng Wireshark để bắt và phân tích các gói tin:.....	7
– Sử dụng Network Miner để bắt và phân tích các gói tin:.....	9
III. Tài liệu tham khảo: .....	10

## I. Tìm hiểu lý thuyết:

### – tcpdump:

- tcpdump là một công cụ phân tích gói tin mạng chạy dưới giao diện dòng lệnh (CLI). Nó cho phép người dùng hiển thị các gói tin TCP/IP đang được truyền hoặc nhận qua mạng mà máy tính chạy tcpdump kết nối tới.
- tcpdump có mặt trên Windows và các hệ điều hành họ Unix như Linux, BSD, MacOS, OpenWRT, v.v
- Một số tác dụng của tcpdump (và các công cụ bắt gói tin nói chung) trên thực tế:
- Giám sát hạ tầng mạng để phát hiện các kết nối bất thường.
- Tấn công ăn trộm tên tài khoản, mật khẩu và các thông tin nhạy cảm khác nếu dữ liệu được truyền qua HTTP không mã hoá.
- Kiểm tra lỗi trên hạ tầng mạng (định tuyến sai, cổng đóng, v.v).
- tcpdump có thể lưu kết quả bắt gói tin vào tệp pcap.

### – Wireshark:

- Wireshark là một công cụ phân tích gói tin mạng mã nguồn mở và miễn phí, được sử dụng rộng rãi trên thế giới. Wireshark có mặt trên Windows và các hệ điều hành họ Unix.
- Khác với tcpdump, Wireshark có giao diện đồ hoạ (GUI) giúp người dùng dễ tương tác hơn.
- Wireshark khá giống với tcpdump. Một số tính năng của Wireshark liệt kê dưới đây cũng có mặt trên tcpdump:
- Hỗ trợ nhiều giao thức mạng khác nhau.
- Giám sát hạ tầng mạng trên thời gian thực.
- Bắt các gói tin trên thời gian thực, có thể lưu lại và kiểm tra sau.
- Hỗ trợ đọc ghi nhiều loại tệp dữ liệu: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, v.v
- Hỗ trợ phân tích VoIP.

- Có thể xuất dữ liệu dưới dạng XML, PostScript, CSV hoặc plain text.
- NetworkMiner:
  - NetworkMiner là một công cụ phân tích mạng (NFAT) mã nguồn mở dành cho Windows.
  - Tương tự như tcpdump và Wireshark, NetworkMiner có thể được sử dụng như một công cụ bắt / dò tìm gói tin mạng thụ động để phát hiện hệ điều hành, phiên, tên máy chủ, cổng đang mở, v.v. mà không đặt bất kỳ lưu lượng nào trên mạng.
  - NetworkMiner có thể lưu kết quả bắt gói tin vào tệp pcap.

## II. Mô tả cài đặt & kết quả:

- Sử dụng tcpdump:
  - Trước hết, sinh viên cấu hình Sniffer gia nhập hai mạng Internal và External. **Internal là eth0, external là eth1.**

```

kali@B21AT012-LongVT-Kali-Sniffer: ~
File Actions Edit View Help
(kali@B21AT012-LongVT-Kali-Sniffer)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
  ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
  roup default qlen 1000
    link/ether 00:0c:29:0d:ce:67 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.129/24 brd 192.168.100.255 scope global dynamic noprefix
  route eth0
        valid_lft 1774sec preferred_lft 1774sec
    inet6 fe80::216e:9b73:20ae:aa45/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
  roup default qlen 1000
    link/ether 00:0c:29:0d:ce:71 brd ff:ff:ff:ff:ff:ff
    inet 10.10.19.131/24 brd 10.10.19.255 scope global dynamic noprefixroute
  eth1
        valid_lft 1774sec preferred_lft 1774sec
    inet6 fe80::8520:e2c1:46b3:3094/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
  
```

- Tiếp theo, chạy **sudo tcpdump -i eth0 icmp -n** để bắt gói tin ping trên mạng internal.

- Thực hiện ping từ Windows Server Internal đến pfSense như hình dưới.

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>echo B21DCAT012_Long_VT
B21DCAT012_Long_VT

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::aa7b:fa12:6499:c1ca%3
    IPv4 Address. . . . . : 192.168.100.201
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1

C:\Users\Administrator>ping 192.168.100.1

Pinging 192.168.100.1 with 32 bytes of data:
Reply from 192.168.100.1: bytes=32 time=1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time=1ms TTL=64
Reply from 192.168.100.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

- Kết quả, tcpdump bắt được các gói tin, trong đó xen kẽ là gói tin ping gửi từ Windows Server Internal địa chỉ 192.168.100.201 đến pfSense 192.168.100.1 và gói tin trả lời từ pfSense đến Windows Server Internal.

```
kali@B21AT012-LongVT-Kali-Sniffer: ~  
File Actions Edit View Help  
  
(kali@B21AT012-LongVT-Kali-Sniffer)-[~]  
$ sudo tcpdump -i eth0 icmp -n  
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
05:14:40.205057 IP 192.168.100.1 > 192.168.100.201: ICMP host 192.168.206.2 u  
nreachable, length 88  
05:15:05.098822 IP 192.168.100.201 > 192.168.100.1: ICMP echo request, id 1,  
seq 9, length 40  
05:15:05.099289 IP 192.168.100.1 > 192.168.100.201: ICMP echo reply, id 1, se  
q 9, length 40  
05:15:06.112568 IP 192.168.100.201 > 192.168.100.1: ICMP echo request, id 1,  
seq 10, length 40  
05:15:06.113033 IP 192.168.100.1 > 192.168.100.201: ICMP echo reply, id 1, se  
q 10, length 40  
05:15:07.128626 IP 192.168.100.201 > 192.168.100.1: ICMP echo request, id 1,  
seq 11, length 40  
05:15:07.129664 IP 192.168.100.1 > 192.168.100.201: ICMP echo reply, id 1, se  
q 11, length 40  
05:15:08.143963 IP 192.168.100.201 > 192.168.100.1: ICMP echo request, id 1,  
seq 12, length 40  
05:15:08.144747 IP 192.168.100.1 > 192.168.100.201: ICMP echo reply, id 1, se  
q 12, length 40  
^C  
9 packets captured  
9 packets received by filter  
0 packets dropped by kernel
```

- Thực hiện tương tự với mạng External và cũng bắt được các gói tin trao đổi giữa Windows Server External 10.10.19.202 và 10.10.19.1.

```
Administrator: C:\Windows\system32\cmd.exe  
  
C:\Users\Administrator>echo B21DCAT012_Long_VT  
B21DCAT012_Long_VT  
  
C:\Users\Administrator>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::ef59:a0b3:9f28:e076%5  
IPv4 Address. . . . . : 10.10.19.202  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.10.19.1  
  
C:\Users\Administrator>ping 10.10.19.1  
  
Pinging 10.10.19.1 with 32 bytes of data:  
Reply from 10.10.19.1: bytes=32 time=2ms TTL=64  
Reply from 10.10.19.1: bytes=32 time=1ms TTL=64  
Reply from 10.10.19.1: bytes=32 time<1ms TTL=64  
Reply from 10.10.19.1: bytes=32 time=1ms TTL=64  
  
Ping statistics for 10.10.19.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

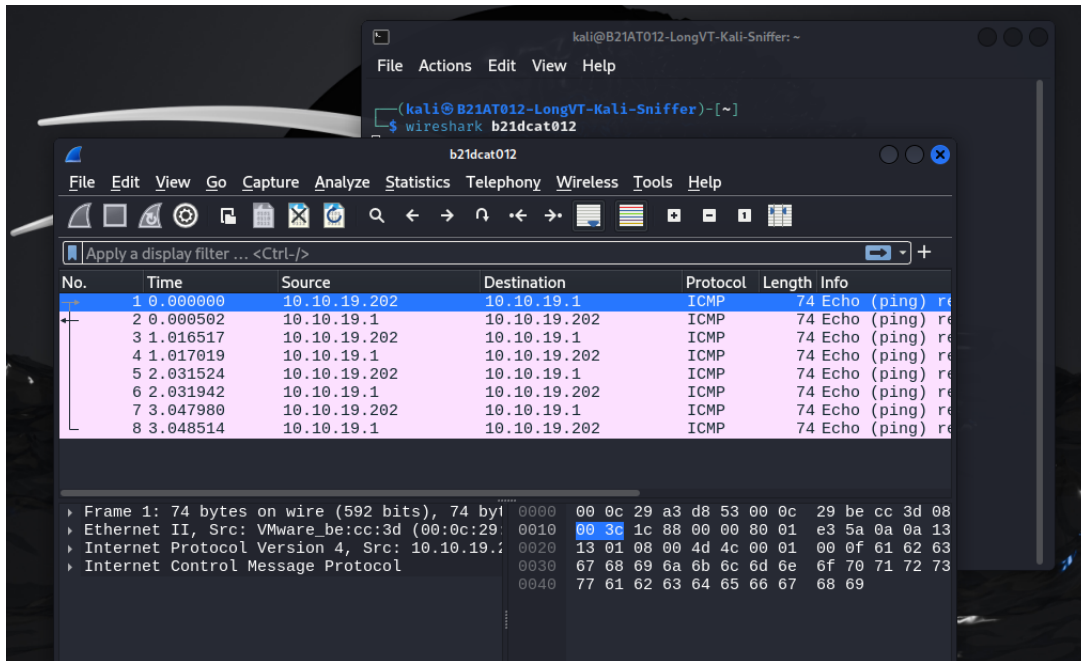
```
kali@B21AT012-LongVT-Kali-Sniffer: ~
File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-Sniffer)-[~]
$ sudo tcpdump -i eth1 icmp -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
05:02:28.351910 IP 10.10.19.202 > 10.10.19.1: ICMP echo request, id 1, seq 5, l
length 40
05:02:28.351911 IP 10.10.19.1 > 10.10.19.202: ICMP echo reply, id 1, seq 5, l
length 40
05:02:29.370926 IP 10.10.19.202 > 10.10.19.1: ICMP echo request, id 1, seq 6,
length 40
05:02:29.371771 IP 10.10.19.1 > 10.10.19.202: ICMP echo reply, id 1, seq 6, l
length 40
05:02:30.386231 IP 10.10.19.202 > 10.10.19.1: ICMP echo request, id 1, seq 7,
length 40
05:02:30.386677 IP 10.10.19.1 > 10.10.19.202: ICMP echo reply, id 1, seq 7, l
length 40
05:02:31.417856 IP 10.10.19.202 > 10.10.19.1: ICMP echo request, id 1, seq 8,
length 40
05:02:31.418301 IP 10.10.19.1 > 10.10.19.202: ICMP echo reply, id 1, seq 8, l
length 40
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
```

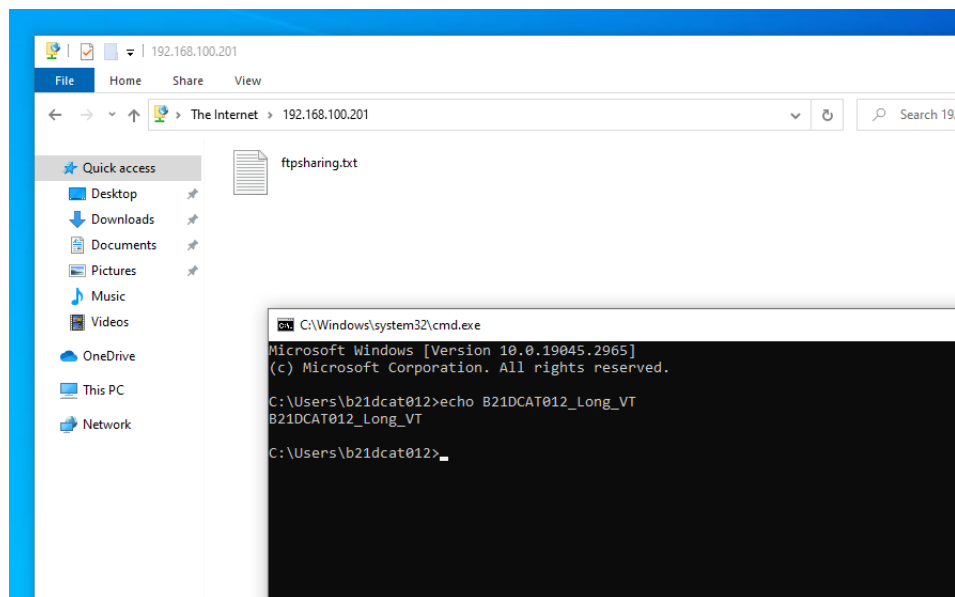
- Để lưu kết quả vào file, dùng lệnh **sudo tcpdump -i eth1 icmp -w <tênfile>**

```
(kali@B21AT012-LongVT-Kali-Sniffer)-[~]
$ sudo tcpdump -i eth1 icmp -n -w b21dcat012
tcpdump: listening on eth1, link-type EN10MB (Ethernet), snapshot length 2621
44 bytes
^C8 packets captured
8 packets received by filter
0 packets dropped by kernel
```

- File này sau đó có thể được mở bằng Wireshark như hình dưới.

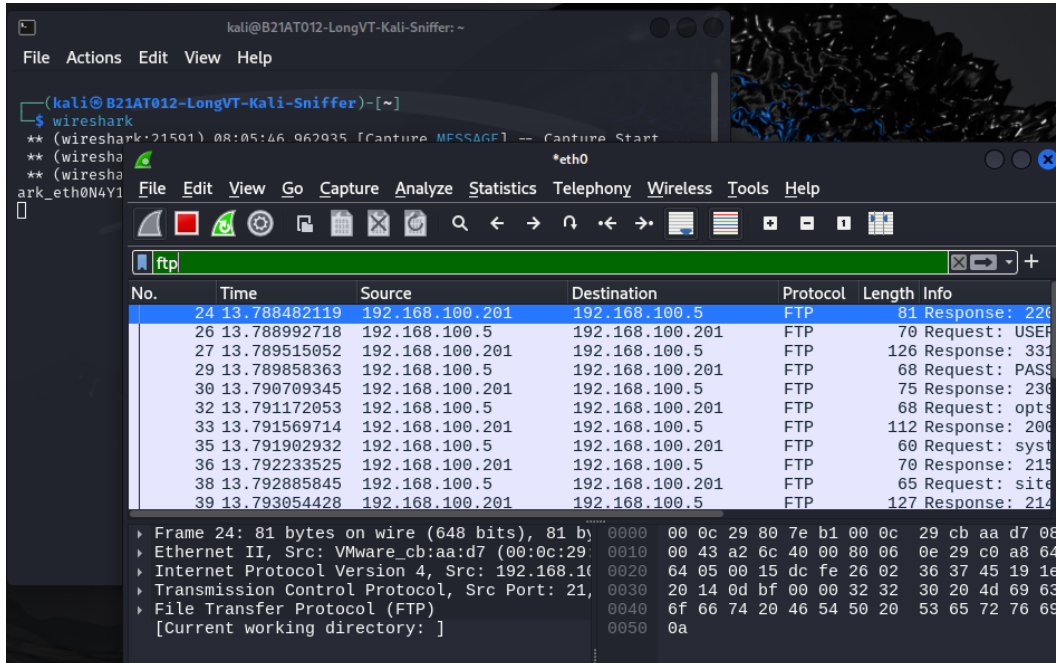


- Sử dụng Wireshark để bắt và phân tích các gói tin:
- Khởi động Wireshark trên Sniffer, chọn interface là eth0 rồi bấm Start capture.
- Khởi động Windows 10 attack rồi dùng gõ ftp://192.168.100.201 để truy cập nội dung thư mục FTP của Windows Server Internal.

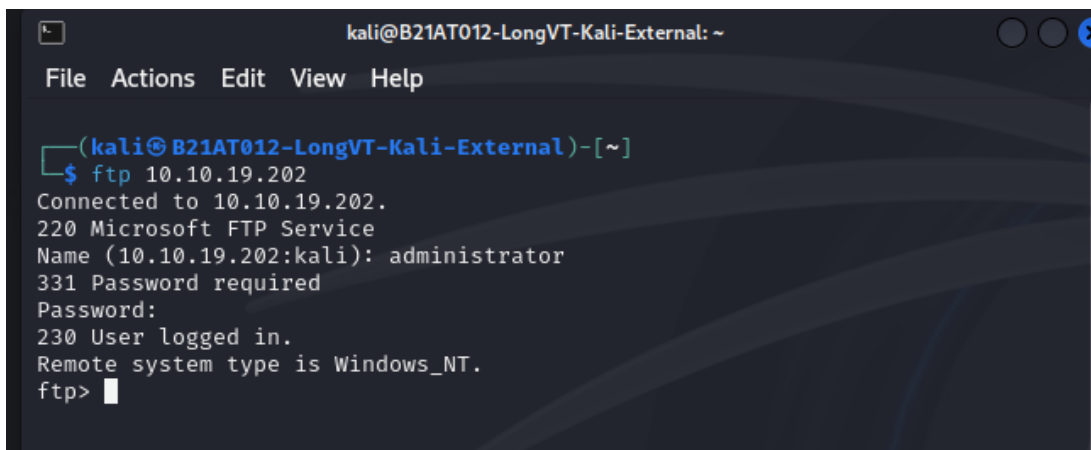




- Kết quả, Wireshark bắt được các gói tin ftp như hình dưới. 192.168.100.5 là địa chỉ IP của Windows 10, còn 192.168.100.201 là địa chỉ IP của Windows Server Internal.
- User anonymous và password là tên đăng nhập mặc định của FTP, do sinh viên đã cấu hình máy chủ FTP chấp nhận người dùng ẩn danh (anonymous).



- Tiếp theo, khởi động lại Wireshark rồi chọn capture giao diện là eth1.

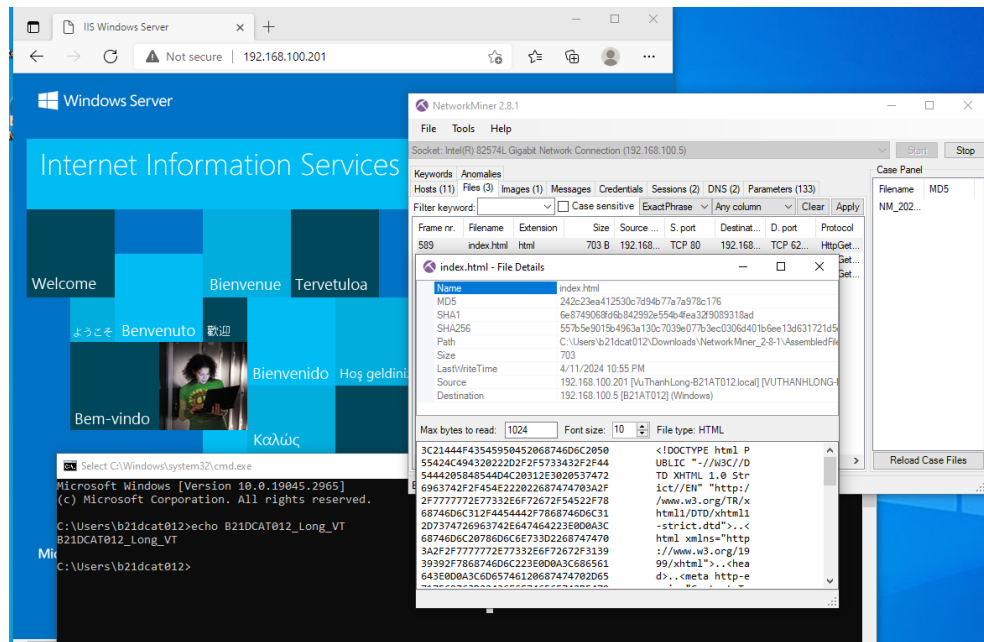


- Kết quả, thu được các gói tin ftp tương tự

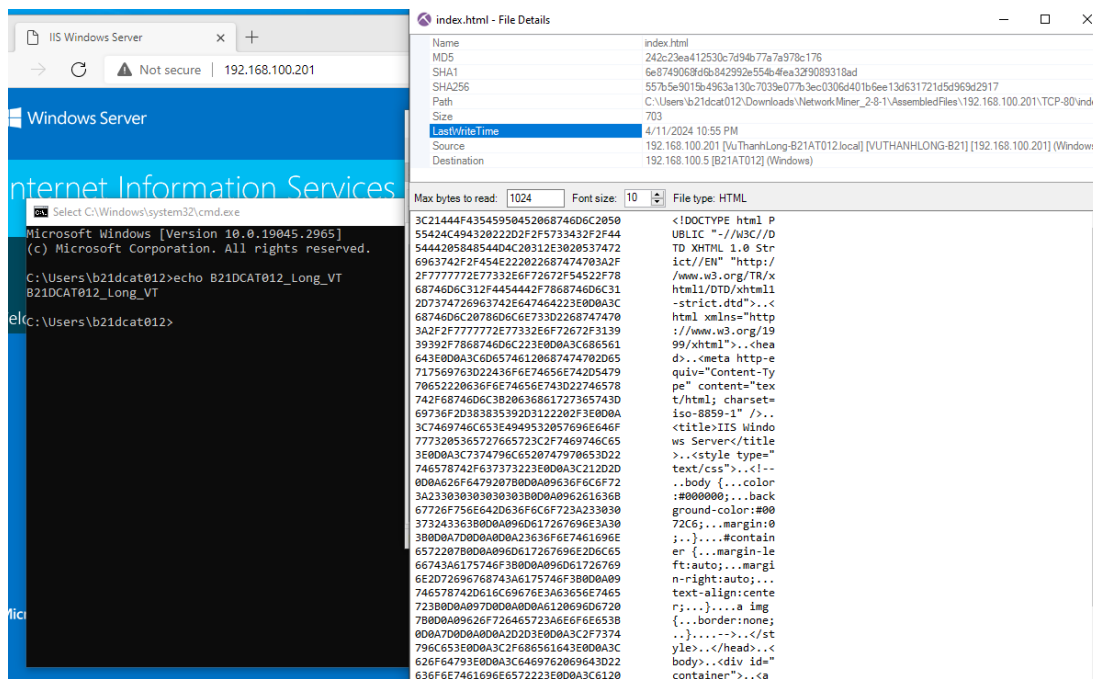
No.	Time	Source	Destination	Protocol	Length	Info
4	0.001583506	10.10.19.202	10.10.19.148	FTP	81	Response: 220
10	13.527770532	10.10.19.148	10.10.19.202	FTP	74	Request: USER
11	13.527991344	10.10.19.202	10.10.19.148	FTP	77	Response: 331
34	30.465495534	10.10.19.148	10.10.19.202	FTP	76	Request: PASS
36	30.488822620	10.10.19.202	10.10.19.148	FTP	75	Response: 230
38	30.489304936	10.10.19.148	10.10.19.202	FTP	60	Request: SYST
39	30.489409470	10.10.19.202	10.10.19.148	FTP	70	Response: 215
40	30.490116983	10.10.19.148	10.10.19.202	FTP	60	Request: FEAT
41	30.490487927	10.10.19.202	10.10.19.148	FTP	88	Response: 211
42	30.490488067	10.10.19.202	10.10.19.148	FTP	72	Response: LA
43	30.490488107	10.10.19.202	10.10.19.148	FTP	107	Response: AL

▶ Frame 4: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface eth1  
 ▶ Ethernet II, Src: VMware\_b8:00:00:00:00:00 (08:00:00:00:00:00), Dst: 10.10.19.148 (08:00:00:00:00:00)  
 ▶ Internet Protocol Version 4, Src: 10.10.19.202, Dst: 10.10.19.148  
 ▶ Transmission Control Protocol, Src Port: 21, Dst Port: 21  
 ▶ File Transfer Protocol (FTP)  
 [Current working directory: ]

- Sử dụng Network Miner để bắt và phân tích các gói tin:
- Trước hết tải và giải nén Network Miner. Sinh viên chạy NetworkMiner.exe với quyền quản trị viên.
- Lựa chọn interface là Socket: Intel® PRO/1000MT Network Connection(192.168.100.5) rồi bấm Start để bắt đầu bắt các gói tin.
- Truy cập <http://192.168.100.201> trên trình duyệt để mở trang web mặc định của máy chủ Windows Server Internal.
- Kết quả, bắt được tệp index.html như hình dưới.



- Thông tin cụ thể của tệp index.html ở hình dưới.



### III. Tài liệu tham khảo:

tcpdump manpage: <https://www.tcpdump.org/manpages/>

Wireshark documentation: [https://www.wireshark.org/docs/wsug\\_html\\_chunked/](https://www.wireshark.org/docs/wsug_html_chunked/)