

សារី ក្នុងវិនិយោគ (62010684)

(3)

The Wireshark interface shows a list of network packets. The columns include Time, Source, Destination, Protocol, Length, HTTP Data, and Info. The Info column displays various FTP commands such as OPTS, USER, PASS, and PORT. The packet list spans from 8889 to 73742, with many entries from 192.168.1.6 to 192.168.1.5.

```

Frame 8889: 31 bytes captured (480 bits) on interface 'Intel(R) Dual Band Wireless-AC 7265 (phy0) (mon0)' at 2020-01-27 14:22:16.000000 UTC (0.000 seconds in base 1000)
Ethernet II, Src: Router [00:0c:29:b4:4f:01], Dst: Intel(R) Dual Band Wireless-AC 7265 [192.168.1.6]
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.5
Transmission Control Protocol, Src Port: 21, Dst Port: 63404, Seq: 1, Ack: 1, Len: 27
File Transfer Protocol (FTP)
[Current working directory: ]
```

Frame 8890: 34 bytes captured (480 bits) on interface 'Intel(R) Dual Band Wireless-AC 7265 (phy0) (mon0)' at 2020-01-27 14:22:16.000000 UTC (0.000 seconds in base 1000)
Ethernet II, Src: Router [00:0c:29:b4:4f:01], Dst: Intel(R) Dual Band Wireless-AC 7265 [192.168.1.6]
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.5
Transmission Control Protocol, Src Port: 21, Dst Port: 63404, Seq: 1, Ack: 1, Len: 27
File Transfer Protocol (FTP)
[Current working directory:]



Wireshark

The terminal window shows the command 'ftp test.rebeex.net' being run. The session connects to the host and lists the contents of the directory. The file 'test.rebeex.net' is transferred successfully.

```

C:\Select Command Prompt - ftp test.rebeex.net
Microsoft Windows [Version 10.0.19041.746]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\ftp> test.rebeex.net
Connected to test.rebeex.net.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (test.rebeex.net:(none)): demo
331 Password required for demo.
Password:
230 User logged in.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection.
226 Transfer complete.
```

Command prompt. →

4

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp-data

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Host	Info
73739	269.822556	195.144.107.198	192.168.1.6	FTP-DA...	149			FTP Data: 95 bytes (P)

```

> Frame 73739: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{6E015E2C-04DF-4EDD-920A-DA
< Ethernet II, Src: Netcore_9b:ca:b2 (e4:be:ed:9b:ca:b2), Dst: IntelCor_a2:ea:72 (34:e1:2d:a2:ea:72)
> Destination: IntelCor_a2:ea:72 (34:e1:2d:a2:ea:72)
> Source: Netcore_9b:ca:b2 (e4:be:ed:9b:ca:b2)
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 195.144.107.198, Dst: 192.168.1.6
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSSCP: CS0, ECN: Not-ECT)
  Total Length: 135
  Identification: 0x7f14 (32532)
> Flags: 0x40, Don't fragment
  Fragment Offset: 0
  Time to Live: 110
  Protocol: TCP (6)
  Header Checksum: 0x9c57 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 195.144.107.198
  Destination Address: 192.168.1.6
> Transmission Control Protocol, Src Port: 20, Dst Port: 63368, Seq: 1, Ack: 1, Len: 95
  Source Port: 20
  Destination Port: 63368
  [Stream index: 51]
  [TCP Segment Len: 95]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 3646419670
  [Next Sequence Number: 96 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 871537338
  0101 .... = Header Length: 20 bytes (5)
> Flags: 0x0108 (PSH, ACK)
  Window: 258
  [Calculated window size: 66048]
  [Window size scaling factor: 256]
  Checksum: 0x9dae [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [timestamps]
  TCP payload: (95 bytes)
  FTP Data (95 bytes data)
  [Setup frame: 73063]
  [Setup method: PORT]
  [Command: LIST]
  [Current working directory: ]
  > Line-based text data (2 lines)

0020 01 06 00 14 f7 88 d9 57 f2 d6 33 f2 9a ba 50 18 .....W - 3...P
0030 01 02 9d ae 00 00 31 30 2d 31 39 2d 32 30 20 20 .....10 - 19-20
0040 30 33 3a 31 39 58 4d 20 20 20 20 20 20 3c 44 03:19PM <D

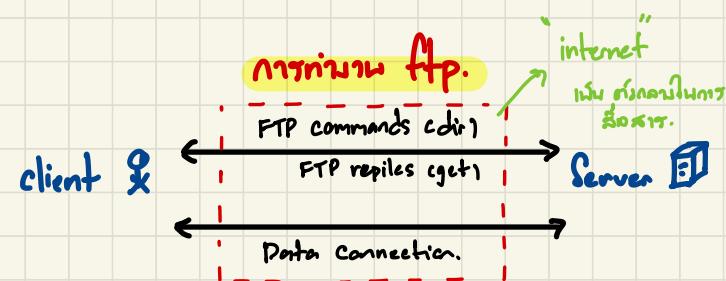
```

Destination Port (tcp.dstport), 2bytes | Packets: 78368 | Displayed: 1 (0.0%) · Marked: 1 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

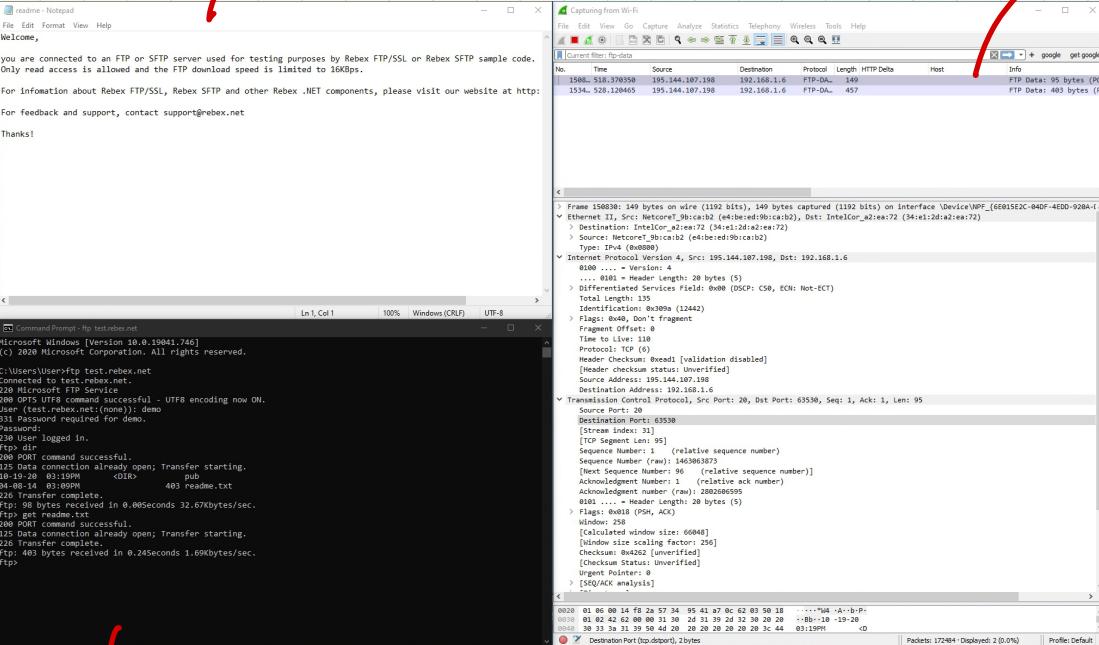
Q packet nr: 73,739

source port: 20

destination port: 63,368



(5)



6

READMEOFROMWIRESHARK - Notepad

Welcome,

you are connected to an FTP or SFTP server used for testing purposes by Rebex FTP/SSL or Rebex SFTP sample code.
Only read access is allowed and the FTP download speed is limited to 16Kbps.

For information about Rebex FTP/SSL, Rebex SFTP and other Rebex .NET components, please visit our website at <http://>

For feedback and support, contact support@rebex.net

Thanks!

readme - Notepad

Welcome,

you are connected to an FTP or SFTP server used for testing purposes by Rebex FTP/SSL or Rebex SFTP sample code.
Only read access is allowed and the FTP download speed is limited to 16Kbps.

For information about Rebex FTP/SSL, Rebex SFTP and other Rebex .NET components, please visit our website at <http://>

For feedback and support, contact support@rebex.net

Thanks!

Visluminojū
#

7.

Wireshark - Follow TCP Stream (tcp.stream eq 0) - [no capture file]

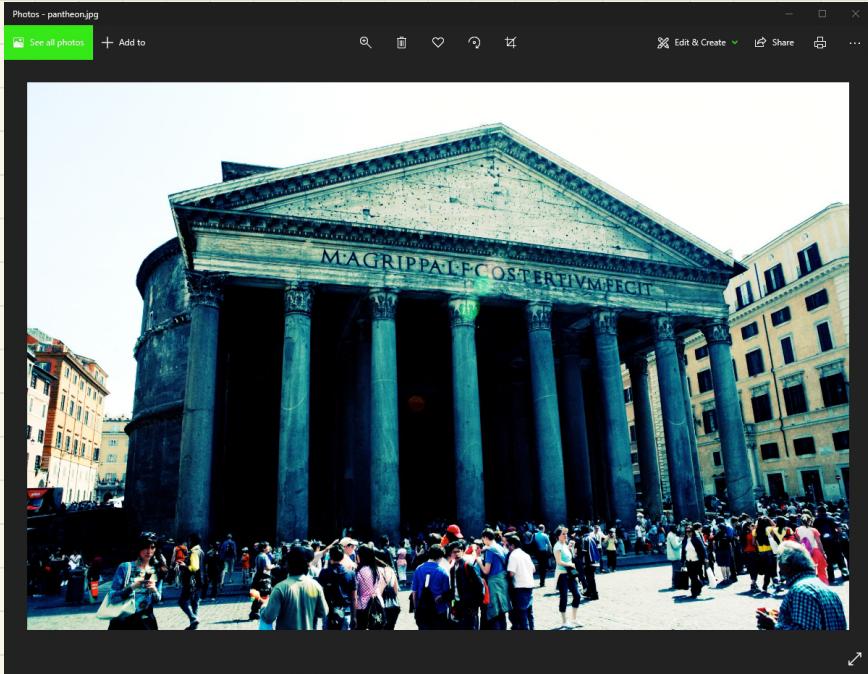
```

220 (vsFTPd 2.0.3)
USER anonymous
331 Please specify the password.
PASS anypwd
230 Login successful.
PORT 192,168,0,101,206,177
200 PORT command successful. Consider using PASV.
NLST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,0,101,206,178
200 PORT command successful. Consider using PASV.
RETR pantheon.jpg
150 Opening BINARY mode data connection for pantheon.jpg (5544612 bytes).
226 File send OK.
QUIT
221 Goodbye.

```

1. USER nimr login សារិយវិធាន (anonymous)
2. PASS ពាក្យសម្បត្តិការណ (anonymous ទៅលើគ្រប់គ្រង)
3. PORT សំណើរចនាអំពីរាងដឹងការណ ដែលមិនមែន Port 20
4. NLST ជួយដាក់ឱ្យរីករាយ។
5. TYPE បង្ហាញរូបរាង (I = Image)
6. RETR nimr ដែលសារិយវិធាន FTP Server (pantheon.jpg)
7. QUIT disconnect នៃ FTP Server.

- 8) display filter ԱՆՈ՞Ր : (tcp.stream eq 0)
- 9) pantheon.jpg.



- 10) ԱՌԱՎԱՐԱՐՈՒԹՅՈՒՆ

11.3

↳ zip cıktıları

 1.328233 Seconds. ~~#~~

• Lip C

និង → Set time reference 1 in packet នៃការទូរសព្ទ download (សម្រាប់ការបង្កើត) ហើយ packet នៃ 16 រាល់នៅលើការទូរសព្ទ download.

nsl.kmitl.ac.th

133

DNS Cemetery:

Question: 1

www.ce.kmitl.ac.th type A.

DNS Response:

Question : 1
www. cc. fumit. ac. in type CNAME.

14.

Query :

Question : 1

Answers Pt: 0

229.4.241.161 in-addr.arpa type PTR class IN.

Response:

Question : 1

Answers Pt. 1

119.4.246.161 in-addr.arpa type PTR class IN.

jeweler19.cc.kmifl.ac.th

(15)

```
Command Prompt - nslookup
: 199.7.91.13
server: d.root-servers.net
address: 199.7.91.13

+-----+
| In-addr.arpa      nameserver = a.in-addr-servers.arpa
| In-addr.arpa      nameserver = b.in-addr-servers.arpa
| In-addr.arpa      nameserver = c.in-addr-servers.arpa
| In-addr.arpa      nameserver = d.in-addr-servers.arpa
| In-addr.arpa      nameserver = e.in-addr-servers.arpa
| In-addr.arpa      nameserver = f.in-addr-servers.arpa
| .in-addr-servers.arpa internet address = 199.198.182.53
| .in-addr-servers.arpa internet address = 199.253.183.183
| .in-addr-servers.arpa internet address = 196.216.169.10
| .in-addr-servers.arpa internet address = 260.10.60.53
| .in-addr-servers.arpa internet address = 203.119.86.101
| .in-addr-servers.arpa internet address = 193.0.9.1
| .in-addr-servers.arpa AAAA IPv6 address = 2620:37:0000::53
| .in-addr-servers.arpa AAAA IPv6 address = 2001:500:87::87
| .in-addr-servers.arpa AAAA IPv6 address = 2001:43F8:110:10
| .in-addr-servers.arpa AAAA IPv6 address = 2001:13C7:7010::53
| .in-addr-servers.arpa AAAA IPv6 address = 2001:dd8:6::161
| .in-addr-servers.arpa AAAA IPv6 address = 2001:67c:e0::1
*** No internal type for both IPV4 and IPV6 Addresses (A+AAAA) record
```

(16)

```
Command Prompt - nslookup
address: 199.7.91.13
www.ce.kmitl.ac.th
server: d.root-servers.net
address: 199.7.91.13

Name: www.ce.kmitl.ac.th
Served by:
a.thains.co.th
 122.155.23.64
 2001:c00:4618:3000::30
th
b.thains.co.th
 203.159.64.64
 2001:c00:4618:3000::30
th
c.thains.co.th
 194.0.1.28
 2001:678:4::1c
th
p.thains.co.th
 204.61.216.126
 2001:500:14:6126:ad::1
th
ns.thnic.net
 202.28.0.1
th
```

d.root-servers.net.

```
Command Prompt - nslookup
*** Can't find address for server ns.thnic.net: Non-authoritative answer
+-----+
| In-addr.arpa      nameserver = a.in-addr-servers.arpa
| In-addr.arpa      nameserver = b.in-addr-servers.arpa
| In-addr.arpa      nameserver = c.in-addr-servers.arpa
| In-addr.arpa      nameserver = d.in-addr-servers.arpa
| In-addr.arpa      nameserver = e.in-addr-servers.arpa
| In-addr.arpa      nameserver = f.in-addr-servers.arpa
| .in-addr-servers.arpa Internet address = 199.198.182.53
| .in-addr-servers.arpa Internet address = 199.253.183.183
| .in-addr-servers.arpa Internet address = 196.216.169.10
| .in-addr-servers.arpa Internet address = 260.10.60.53
| .in-addr-servers.arpa Internet address = 203.119.86.101
| .in-addr-servers.arpa AAAA IPv6 address = 2620:37:0000::53
| .in-addr-servers.arpa AAAA IPv6 address = 2001:500:87::87
| .in-addr-servers.arpa AAAA IPv6 address = 2001:43F8:110:10
| .in-addr-servers.arpa AAAA IPv6 address = 2001:13C7:7010::53
| .in-addr-servers.arpa AAAA IPv6 address = 2001:dd8:6::161
| .in-addr-servers.arpa AAAA IPv6 address = 2001:67c:e0::1
Server: [202.28.0.1]
Address: 202.28.0.1

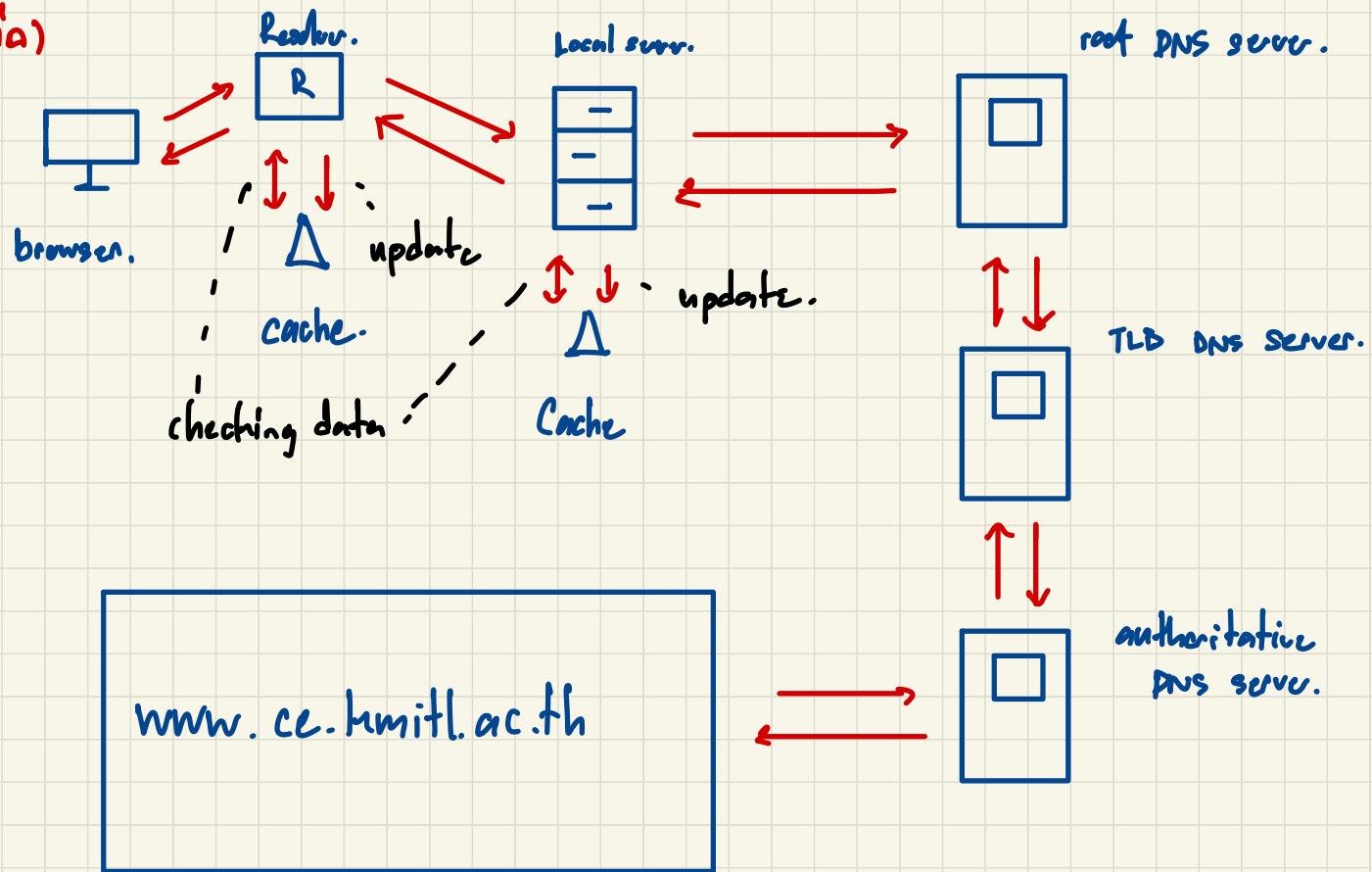
Name: acth
> kmitl.ac.th
Server: [202.28.0.1]
Address: 202.28.0.1

Name: kmitl.ac.th
Address: 163.246.34.11

> ce.kmitl.ac.th
Server: [202.28.0.1]
Address: 202.28.0.1

Name: ce.kmitl.ac.th
Served by:
- ns1.kmitl.ac.th
 161.246.52.21
ce.kmitl.ac.th
diamond.ce.kmitl.ac.th
 161.246.4.3
ce.kmitl.ac.th
```

(18.) (cont'd)



(18.) Packet n° 11

14.7

DNS Delta , Server query , www.ce.kmitl.ac.th.

161.246.4.5
(0.00331 sec)

< 161.246.52.21
(0.01968 sec)

< 8.8.8.8
(0.032494 sec)

