

PR Lab 6

Protocol Description by reverse engineering using WireShark

BizdigaStas FAF-151

Identifying packets:

By the teacher's tip, the protocol to look out for is udp, and as it's written down in the filters, we can see the following:

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The packet list pane shows a table of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The filter bar at the top of the packet list is set to 'udp'. The packet details pane shows the selected packet (No. 171) with its structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (172 bytes).

No.	Time	Source	Destination	Protocol	Length	Info
2...	257.39...	10.35.131.139	230.185.192.108	UDP	226	60190 → 42424 Len=184
2...	257.38...	10.35.131.139	230.185.192.108	UDP	178	42424 → 42424 Len=136
1...	212.07...	10.35.131.65	230.185.192.108	UDP	218	50261 → 42424 Len=176
1...	212.06...	10.35.131.65	230.185.192.108	UDP	218	50260 → 42424 Len=176
1...	211.77...	10.35.131.139	230.185.192.108	UDP	182	36976 → 42424 Len=140
1...	171.98...	10.35.131.139	230.185.192.108	UDP	214	45903 → 42424 Len=172
2...	297.58...	18.184.56.218	10.35.131.187	TLSv1.2	117	Application Data
2...	297.54...	18.184.56.218	10.35.131.187	TLSv1.2	115	Application Data

> Frame 1567: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0
> Ethernet II, Src: LiteonTe_b0:0f:c1 (ac:b5:7d:b0:0f:c1), Dst: IPv4mcast_39:c0:6c (01:00:5e:39:c0:6c)
> Internet Protocol Version 4, Src: 10.35.131.139, Dst: 230.185.192.108
> User Datagram Protocol, Src Port: 45903, Dst Port: 42424
> Data (172 bytes)

These are likely, messages from the other users on the app already. Let's try log in and see what happens...

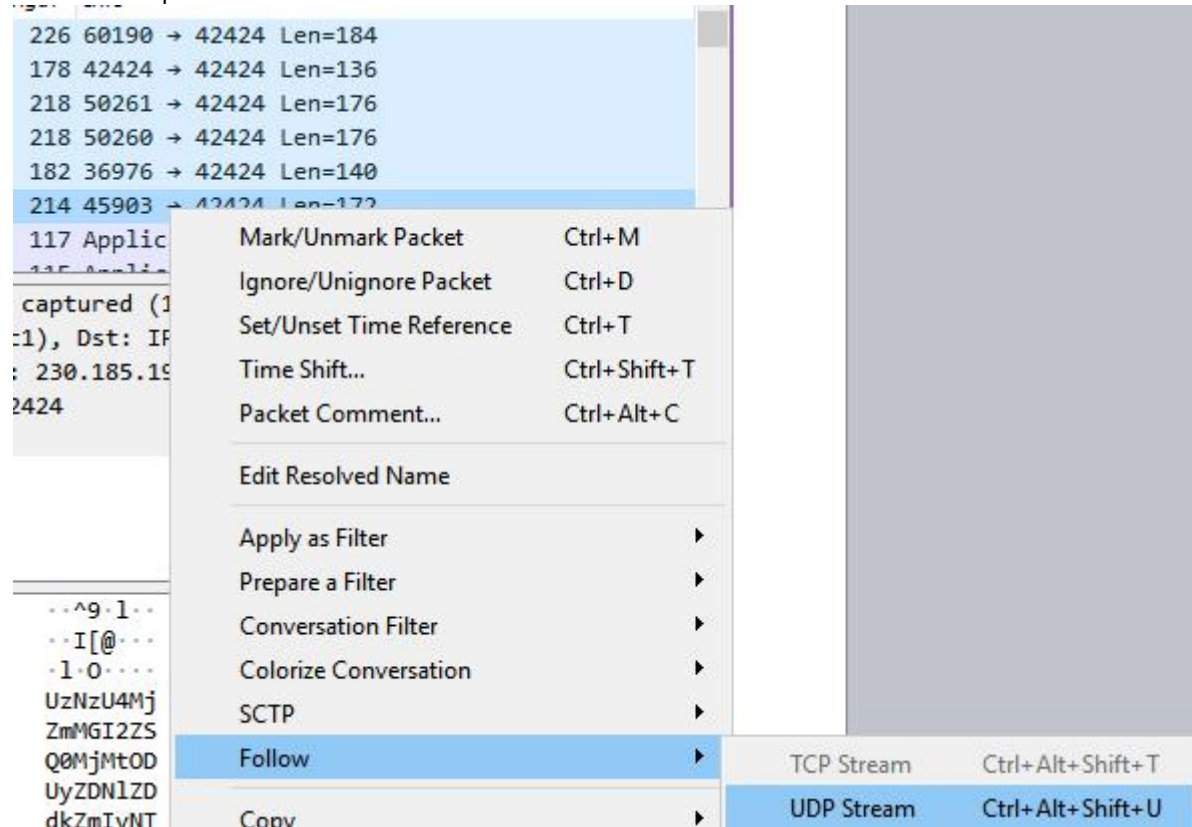
Join

Username * TheGodAllMighty

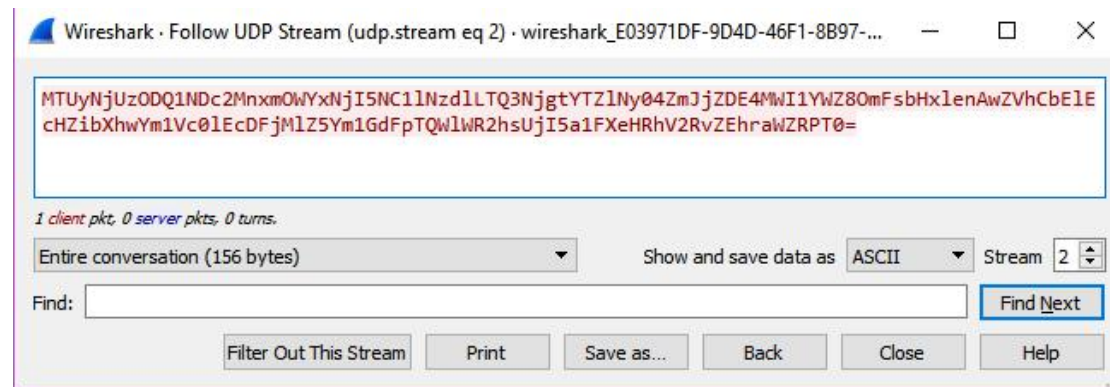
Join

But before that, It would be nice to filter the other unnecessary packets by adding:
'udp.port == 42424'

To follow the packets easier we can do this:



Which leads to:



This looks like a base64 encoded string, so as i decode it, this is the answer:

Decode from Base64 format

Simply use the form below

MTUyNjUzODQ1NDc2MnxmOWYxNjI5NC1INzdILTQ3NjgtYTZlNy04ZmJjZDE4MWI1YWZ8OmFsbHxlenAwZVhCbEIEcHZibXhwYm1Vc0IEcDFjMlZ5Ym1GdFpTQWlWR2hsUjl5a1FXeHRhV2RvZEhraVZRPT0=

< DECODE >

UTF-8

You may also select input charset.

☒ Live mode ON

Decodes while you type or paste (strict format).

Note that decoding of binary data (like images, documents, etc.) does not work in live mode.

Decodes an entire file (max. 10MB).

1526538454762|9f16294-e77e-4768-a6e7-8fbc181b5af|all|ezp0eXBllDpvmxpbmUslDp1c2VybmFtZSAiVGhlR29kQWxtaWdodHkifQ==

Then I take the last part (| are delimiting the parts) and decode it again.

Decode from Base64 format

Simply use the form below

ezp0eXBllDpvmxpbmUslDp1c2VybmFtZSAiVGhlR29kQWxtaWdodHkifQ==

< DECODE >

UTF-8

You may also select input charset.

☒ Live mode ON

Decodes while you type or paste (strict format).

Note that decoding of binary data (like images, documents, etc.) does not work in live mode.

Decodes an entire file (max. 10MB).

{:type :online, :username "TheGodAlmighty"}

And I get the message from the system, telling that my user is now online.

After a bit of analysis I came to the conclusion that the first number,
aka:

1526538454762

is the time in milliseconds, this current value is Thu May 17 2018 9:27:34GMT+0300.

Milliseconds

1526538454762

↕

Convert to Date

Now

Thu 17 May 2018

09:27:34

Next, is the uuid of the sender and receiver.
 f9f16294-e77e-4768-a6e7-8fbcd181b5af - sender
 :all - receiver

i.e. all receive this message, that my user is online.

Another example of message is when it is sent. Following the same procedure, we arrive at the same kind of result:

TheGodAlmighty - LocalChat

Chats

Alexxxiiii

10 minutes

m1

16 minutes

sm

5 minutes

(sending message)

God has aspoken to thou.

Thu May 17 2018 09:43:19 GMT+0300 (GTB Daylight Time)

4	0.807676	10.35.131.187	230.185.192.108	UDP	246 56688 → 42424	Len=204
5	0.818935	10.35.131.94	230.185.192.108	UDP	194 65481 → 42424	Len=152

we get 2 packets

one contains the message and the other one the acknowledgement - a kind of notification that it was delivered.

```
MTUyNjUzOTM5OTI1MHxmOWYxNjI5NC1INzdILTQ3NjgtYTZINy04ZmJjZDE4MWI1YWZ8NzVjZjk0YzEtMTA1IWEJJsSURwamFHRjBMQ0E2ZEhoMEIDSkhiMIFnYUdGeklHRnpjRzlyWlc0Z2RHOGdkR2h2ZFM0aWZRPT0=
```

decoded:

1526539399250 - time in milisec

f9f16294-e77e-4768-a6e7-8fbcd181b5af - sender uuid

75cf94c1-1054-4b4c-8be0-568c1eaba65f - receiver uuid

ezp0eXBIIDpjaGF0LCA6dHh0ICJHb2QgaGFzIGFzcG9rZW4gdG8gdGhvdS4ifQ== - message

message decoded:

{:type :chat, :txt "God has aspoken to thou."}

Next packet:

```
MTUyNjUzOTQwMTU0M3w3NWNmOTRjMS0xMDU0LTRiNGMtOGJlMC01NjhjMWVhYmE2NWZ8ZjlmMTYyOTQtZTc3ZS00NzY4LWE2ZTctOGZiY2QxODFiNWVmfmGV6cDBIWEJJsSURwa1pXeHBkbVZ5WldSOQ==
```

1526539401543 - time
75cf94c1-1054-4b4c-8be0-568c1eaba65f -sender
f9f16294-e77e-4768-a6e7-8fbcd181b5af -receiver
ezp0eXBliIDpkZWxpdmVyZWR9 - msg

message decoded:
{:type :delivered}

Since the protocol is clear we can send a message using wireshark too.
It is done by creating a fake user first:

1. Create our name. The name for new user will be DevilTheWeak. So the message is:
`{:type :online, :username "DevilTheWeak"}`
2. Now we need to encode it to Base64. The result will be
`ezp0eXBliIDpvmxpbmUsIDp1c2VybmFtZSAiRGV2aWxUaGVXZWFrIn0=`
3. We need to rebuild the previous packet structure now: (new time and new uuid)
`1526539999250 | 75cf94c1-1054-4b1c-8be0-568c2eaba66f | :all | ezp0eXBliIDpvmxpbmUsIDp1c2VybmFtZSAiRGV2aWxUaGVXZWFrIn0=`
4. Now we need to encode the contents to Base64:
`MTUyNjUzOTk5OTI1MHw3NWNmOTRjMS0xMDU0LTRiMWMtOGJlMC01NjhjMmVhYmE2NmZ8OmFsbHxlenAwZVhCbElEcHZibXhwYm1Vc0lEcDFjMlZ5Ym1GdFpTQWlSRlYyYVd4VWFHVlhaV0ZySW4wPQ==`
5. We can send the packet now. More of the data that we need can be found in wireshark by looking at the packet, such as : destination ip, port.

Then sending the message:

1. Encoding the text message `{:type :chat, :txt "Are you here?"}` to Base64 :
`ezp0eXBliIDpjaGFOLCA6dHh0ICJBcmUgeW91IGhlcmU/In0=`
2. Getting UUID of our fake user :75cf94c1-1054-4b1c-8be0-568c2eaba66f
3. Finding a UUID for to who send the message, we will use the UUID of the first user we created f9f16294-e77e-4768-a6e7-8fbcd181b5af (god)
4. Making mymessage :
`1526539999950 | 75cf94c1-1054-4b1c-8be0-568c2eaba66f | f9f16294-e77e-4768-a6e7-8fbcd181b5af | ezp0eXBliIDpjaGFOLCA6dHh0ICJBcmUgeW91IGhlcmU/In0=`
5. Encoding it to Base64 :
`MTUyNjUzOTk5OTk1MHw3NWNmOTRjMS0xMDU0LTRiMWMtOGJlMC01NjhjMmVhYmE2NmZ8ZjlmMTYyOTQtZTc3ZS00NzY4LWE2ZTctOGZiY2QxODFiNWFMlHxlenAwZVhCbElEcGphR0YwTENBNmRlaDBJQ0pCY21VZ2VXOTFJR2hsY21VL0luMD0=`
6. Sending it using Packet Sender.

Packet Sender

File Tools Help

Name: test

ASCII: mOTRjMS0xMDU0LTRlMWMtOGJlMmVhYmE2NmZ8OmFsbHxlenAwZVhCbElEcHZibXhwYm1Vc0lEcFjMlZ5Ym1GdFpTQWlSR1YyYVd4VWFHVhaV0ZySW4wPQ==

HEX: 5 63 44 46 6a 4d 6c 5a 35 59 6d 31 47 64 46 70 54 51 57 6c 53 52 31 59 79 59 56 64 34 56 57 46 48 56 6c 68 61 56 30 5a 79 53 57 34 77 50 51 3d 3d

Address: 230.185.192.108 Port: 42424 Resend Delay: 0.0/blank off UDP Send Save

Search Saved Packets... Delete Saved Packet Persistent TCP

Send	Name	Resend (sec)	To Address	To Port	Method	ASCII	Hex
1			230.185.192.108	42424	UDP	MTUyNjUzOTk5OTI1MHw3NWNm...	4d 54 55 79 4e 6a 55 7a 4f 54 6b 35 4f 54 4...

Clear Log Log Traffic Save Log Save Traffic Packet Copy to Clipboard

	Time	From IP	From Port	To IP	To Port	Method	Error	ASCII	Hex
1	10:10:26.259	You	62022	230.185.192.108	42424	UDP		MTUyNjUzOTk5OTI1MHw3NWNm...	4d 54 55 79 4e 6a 55 7a 4f 54 6b 35 4f 54 4...

Then suddenly:

TheGodAlmighty - LocalChat

sm 12 minutes

Delta a few seconds

DevilTheWeak a few seconds

sersunnn 20 minutes

sersunnn 14 minutes

sersunnn 45 minutes

Submit

NEXT MESSAGE:

Packet Sender

File Tools Help

Name: test2

ASCII: hjMmVhYmE2NmZ8ZjlmMTYyOTQtZTc3ZS00NzY4LWE2ZTctOGZlY2QxODFiNWVmIHxlenAwZVhCbElEcGphR0YwTENBNmRlADB3Q0pCY21VZ2VXOTFJR2hsY21VL0luMD0=

HEX: 8 52 30 59 77 54 45 4e 42 4e 6d 52 49 61 44 42 4a 51 30 70 43 59 32 31 56 5a 32 56 58 4f 54 46 4a 52 32 68 73 59 32 31 56 4c 30 6c 75 4d 44 30 3d

Address: 230.185.192.108 Port: 42424 Resend Delay: 0.0/blank off UDP Send Save


Search Saved Packets... Delete Saved Packet Persistent TCP

Send	Name	Resend (sec)	To Address	To Port	Method	ASCII	Hex
1			230.185.192.108	42424	UDP	MTUyNjUzOTk5OTk1MHw3NWNm...	4d 54 55 79 4e 6a 55 7a 4f 54 6b 35 4f 54 6b 3...
2			230.185.192.108	42424	UDP	MTUyNjUzOTk5OTk1MHw3NWNm...	4d 54 55 79 4e 6a 55 7a 4f 54 6b 35 4f 54 49 3...


Clear Log Log Traffic Save Log Save Traffic Packet Copy to Clipboard


	Time	From IP	From Port	To IP	To Port	Method	Error	ASCII	Hex
1	10:12:14.928	You	62022	230.185.192.108	42424	UDP		MTUyNjUzOTk5OTk1MHw3NWNm...	4d 54 55 79 4e 6a 55 7a 4f 54 6b 35 4f 54 6b 3...
2	10:10:26.259	You	62022	230.185.192.108	42424	UDP		MTUyNjUzOTk5OTk1MHw3NWNm...	4d 54 55 79 4e 6a 55 7a 4f 54 6b 35 4f 54 49 3...


Chats


 **Alexxxiiii**
39 minutes

 **m1**
an hour


 **sersunnn**
23 minutes

 **sersunnn**
20 minutes

 **sersun**
26 minutes

 **sm**
14 minutes

 **Delta**
2 minutes

 **DevilTheWeak**
2 minutes

Are you here?

Thu May 17 2018 10:12:14 GMT+0300 (GTB Daylight Time)

It works!!

Creepy.