

Forum:[Hack Forums](#)

Thread: [Anyone know how to figure out .ple encryptions?](#)

qupuf - December 8, 2025, 2:30 pm

I need help reverse engineering the encryption used in Messenger Plus Live LogViewer.exe for .ple (MPLE1 format) files.

What I have:

- LogViewer.exe (native C++, ~3.5MB)
- Dummy .ple file with known password
- Decrypted output for comparison
- Extensive analysis showing it's NOT standard crypto

What I need:

- Python implementation of the password verification/decryption
- OR detailed documentation of the algorithm

I want to run brute or dictionary attacks on the .ple file but right now I'm using a third party software (Logviewer) with its command lines and the PWD/S is really slow, something like 130 and takes days to complete one list such as rockyou

Idk if this goes against TOS but I'm willing to donate for your time...

DramaKing - December 8, 2025, 3:53 pm

Python, especially for nonstandard algorithms, may be only slightly faster than looping a console app.

qupuf - December 8, 2025, 5:15 pm

(Dec 8, 2025 04:53 PM)DramaKing Wrote: [\[CITE\]](#) Python, especially for nonstandard algorithms, may be only slightly faster than looping a console app.

I got it down to about 30 mins for 14 million passwords but the encryption was wrong, multithreaded CPU.

Could get it even faster with hashcat/GPU but have no clue when it comes to encryption and was wondering if someone does.

AbakBarama - December 8, 2025, 6:12 pm

[deleted]f, We can discuss details if your task is still relevant.
[deleted]

The Pact - December 8, 2025, 7:56 pm

(Dec 8, 2025 07:12 PM)AbakBarama Wrote: [\[CITE\]](#) We can discuss details if your task is still relevant.

[deleted]

Sorry the owner of the forum requires that you be an upgraded member of at least Leet before you can put your off-site communication details on the forum. This is at least in part to protect the forum from a lot of dodgy scammers putting their details down.

Glad to have you here! Get those Credibility Ratings up by using the HF Contract system. It's

required for all trades—if someone won't use it, the deal's closed.

qupuf - December 8, 2025, 8:54 pm

(Dec 8, 2025 08:56 PM)The Pact Wrote: [\[CITE\]](#) Sorry the owner of the forum requires that you be an upgraded member of at least Leet before you can put your off-site communication details on the forum. This is at least in part to protect the forum from a lot of dodgy scammers putting their details down.

Glad to have you here! Get those Credibility Ratings up by using the HF Contract system. It's required for all trades—if someone won't use it, the deal's closed.
Could you point me to setting up a HF contract?

qupuf - December 9, 2025, 10:17 pm

[deleted]

Can you help out?

AbakBarama - December 10, 2025, 6:46 am

(Dec 9, 2025 11:17 PM)qupuf Wrote: [\[CITE\]](#) @abakbarama

Can you help out?

Possibly yes.

But we can't exchange contacts and continue discussion privately. As stated above, forum requires money to allow this simple action.

qupuf - December 23, 2025, 7:15 pm

(Dec 10, 2025 07:46 AM)AbakBarama Wrote: [\[CITE\]](#) Possibly yes.

But we can't exchange contacts and continue discussion privately. As stated above, forum requires money to allow this simple action.

I mean, they said it's to protect against dodgy scammers but I can definitely give a review here after we're done. What can I do? I really need this. Contract, whatever works.

m0hx - December 24, 2025, 12:40 am

(Dec 23, 2025 08:15 PM)qupuf Wrote: [\[CITE\]](#) I mean, they said it's to protect against dodgy scammers but I can definitely give a review here after we're done. What can I do? I really need this. Contract, whatever works.

oh good old ple , it was messenger days , i still have some ple log files myself but fortunately i do have the password to decrypt them.

I haven't really thought about breaking/cracking/brute forcing .ple files.

I might give it a shot this weekend. I pretty sure i still have the log viewer app.

send me all details u have about ur attempts or whatever ur findings is in dm or here.

qupuf - December 24, 2025, 10:10 am

(Dec 24, 2025 01:40 AM)m0hx Wrote: [\[CITE\]](#) oh good old ple , it was messenger days , i still have some ple log files myself but fortunately i do have the password to decrypt them.

I haven't really thought about breaking/cracking/brute forcing .ple files.

I might give it a shot this weekend. I pretty sure i still have the log viewer app.

send me all details u have about ur attempts or whatever ur findings is in dm or here.

I did some python scripts with GPT bots, one of them was successful for a dummy .ple file but when I ran a 5 day dictionary attack (rockyou), it was unsuccessful. I want to do more attacks but waiting for days isn't feasible for me.

I had another script that would open a bunch of silent Log Viewer and use all the CPU on them but it was still like 2 days to complete, so I still need something faster. Hashcat with GPU would be amazing.

Let me know what you need!

m0hx - December 24, 2025, 10:51 am

(Dec 24, 2025 11:10 AM)qupuf Wrote: [\[CITE\]](#) I did some python scripts with GPT bots, one of them was successful for a dummy .ple file but when I ran a 5 day dictionary attack (rockyou), it was unsuccessful. I want to do more attacks but waiting for days isn't feasible for me.

I had another script that would open a bunch of silent Log Viewer and use all the CPU on them but it was still like 2 days to complete, so I still need something faster. Hashcat with GPU would be amazing.

Let me know what you need!

If we could figure out what algo/ hash type they use, u could run it with hashcat. I'll look into it soon, but send me the script u made and everything in private message or convo.

I'll do some research about it tonight.

I'd say if not possible to figure it out we could try to make smthn utilizing gpu like hashcat to try brute forcing / mask attacks (basically custom hashcat like tool specifically made for ple files) but idk if I can do that lol.

I'll write back in few days or week whenever I find something I'll keep u updated here.
ok i found my old files, i'll try now!

powershell command to decrypt:

```
& ".\Log Viewer.exe" /decrypt="yourfile.ple" /pwd="yourpassword"
```

=-

Code [h1]Paths - UPDATE THESE[/h1]

```
$viewerPath = "C:\Path\To\Log Viewer.exe"
```

```
$targetFile = "C:\Path\To\your_file.ple"
```

```
$wordlist = "C:\Path\To\passwords.txt"
```

```
$outputFolder = "C:\Path\To\DecryptedResults"
```

[h1]Create output folder if it doesn't exist[/h1]

```
if (!(Test-Path $outputFolder)) { New-Item -ItemType Directory -Path $outputFolder }
```

[h1]Load passwords and process in parallel[/h1]

```
Get-Content $wordlist | ForEach-Object -Parallel {
```

```
    $password = $_
```

```

$viewer = $using:viewerPath
$target = $using:targetFile
$outDir = $using:outputFolder

# Start the process as High Priority
$proc = Start-Process -FilePath $viewer -ArgumentList "/decrypt=""$target"",
"/pwd=""$password"" -PassThru -NoNewWindow
$proc.PriorityClass = "High"

# Wait for the specific attempt to finish
$proc.WaitForExit()

# Log Viewer.exe creates a new file (usually .html or .txt) upon success.
# We check if a new file appeared in the directory to identify the correct password.
$checkSuccess = Get-ChildItem $outDir | Where-Object { $_.LastWriteTime -gt
(Get-Date).AddSeconds(-5) }

if ($checkSuccess) {
    Write-Host "[SUCCESS] Password found: $password" -ForegroundColor Green
    $password | Out-File "$outDir\FOUND_PASSWORD.txt"
    # Optional: Stop all other attempts if one succeeds
    # Get-Process "Log Viewer" | Stop-Process
}
} -ThrottleLimit [int]$env:NUMBER_OF_PROCESSORS

```

=====

I guess our best approach is to bruteforce with list, ill try to code smthn for u to make it as fast as possible!

If the encryption algorithm is reverse-engineered, a GPU implementation could achieve 1000+ attempts/second.

(Dec 8, 2025 03:30 PM)qupuf Wrote: [\[CITE\]](#) I need help reverse engineering the encryption used in Messenger Plus Live LogViewer.exe for .ple (MPLE1 format) files.

What I have:

- LogViewer.exe (native C++, ~3.5MB)
- Dummy .ple file with known password
- Decrypted output for comparison
- Extensive analysis showing it's NOT standard crypto

What I need:

- Python implementation of the password verification/decryption
- OR detailed documentation of the algorithm

I want to run brute or dictionary attacks on the .ple file but right now I'm using a third party software (Logviewer) with its command lines and the PWD/S is really slow, something like 130 and takes days to complete one list such as rockyou

Idk if this goes against TOS but I'm willing to donate for your time...

omg big news im stupid. i found something so soo helpful!! i gotta finsih this all by tonight.

i need u to send me the files asap, specially the log examples u have. so i can help u further. start Convo or private message me.

InterFear - December 25, 2025, 6:25 am

(Dec 24, 2025 11:51 AM)m0hx Wrote: [CITE](#) If we could figure out what algo/ hash type they use, u could run it with hashcat. I'll look into it soon, but send me the script u made and everything in private message or convo.

I'll do some research about it tonight.

I'd say if not possible to figure it out we could try to make smthn utilizing gpu like hashcat to try brute forcing / mask attacks (basically custom hashcat like tool specifically made for ple files) but idk if I can do that lol.

I'll write back in few days or week whenever I find something I'll keep u updated here.
ok i found my old files, i'll try now!

powershell command to decrypt:

```
& ".\Log Viewer.exe" /decrypt="yourfile.ple" /pwd="yourpassword"
```

=-

Code [h1]Paths - UPDATE THESE[/h1]

```
$viewerPath = "C:\Path\To\Log Viewer.exe"
```

```
$targetFile = "C:\Path\To\your_file.ple"
```

```
$wordlist = "C:\Path\To\passwords.txt"
```

```
$outputFolder = "C:\Path\To\DecryptedResults"
```

[h1]Create output folder if it doesn't exist[/h1]

```
if (!(Test-Path $outputFolder)) { New-Item -ItemType Directory -Path $outputFolder }
```

[h1]Load passwords and process in parallel[/h1]

```
Get-Content $wordlist | ForEach-Object -Parallel {
```

```
    $password = $_
```

```
    $viewer = $using:viewerPath
```

```
    $target = $using:targetFile
```

```
    $outDir = $using:outputFolder
```

```
# Start the process as High Priority
```

```
$proc = Start-Process -FilePath $viewer -ArgumentList "/decrypt=""$target""",
```

```
"/pwd=""$password"" -PassThru -NoNewWindow
```

```
$proc.PriorityClass = "High"
```

```
# Wait for the specific attempt to finish
```

```
$proc.WaitForExit()
```

```
# Log Viewer.exe creates a new file (usually .html or .txt) upon success.
```

```
# We check if a new file appeared in the directory to identify the correct password.
```

```
$checkSuccess = Get-ChildItem $outDir | Where-Object { $_.LastWriteTime -gt
```

```
(Get-Date).AddSeconds(-5) }
```

```

if ($checkSuccess) {
    Write-Host "[SUCCESS] Password found: $password" -ForegroundColor Green
    $password | Out-File "$outDir\FOUND_PASSWORD.txt"
    # Optional: Stop all other attempts if one succeeds
    # Get-Process "Log Viewer" | Stop-Process
}
} -ThrottleLimit [int]$env:NUMBER_OF_PROCESSORS

```

=====

I guess our best approach is to bruteforce with list, ill try to code smthn for u to make it as fast as possible!

If the encryption algorithm is reverse-engineered, a GPU implementation could achieve 1000+ attempts/second.

omg big news im stupid. i found something so soo helpful!! i gotta finsih this all by tonight. i need u to send me the files asap, specially the log examples u have. so i can help u further. start Convo or private message me.
Can you share please when you have done.

Or maybe DM me !

m0hx - December 25, 2025, 8:02 am

(Dec 25, 2025 07:25 AM)InterFear Wrote: [\[CITE\]](#) Can you share please when you have done.

Or maybe DM me !

im waiting for OP to reach out so we can test it first.

qupuf - December 25, 2025, 10:45 am

(Dec 24, 2025 11:51 AM)m0hx Wrote: [\[CITE\]](#) If we could figure out what algo/ hash type they use, u could run it with hashcat. I'll look into it soon, but send me the script u made and everything in private message or convo.

I'll do some research about it tonight.

I'd say if not possible to figure it out we could try to make smthn utilizing gpu like hashcat to try brute forcing / mask attacks (basically custom hashcat like tool specifically made for ple files) but idk if I can do that lol.

I'll write back in few days or week whenever I find something I'll keep u updated here.
ok i found my old files, i'll try now!

powershell command to decrypt:

& ".\Log Viewer.exe" /decrypt="yourfile.ple" /pwd="yourpassword"

=-

Code [h1]Paths - UPDATE THESE[/h1]

```
$viewerPath = "C:\Path\To\Log Viewer.exe"
$targetFile = "C:\Path\To\your_file.ple"
$wordlist = "C:\Path\To\passwords.txt"
$outputFolder = "C:\Path\To\DecryptedResults"
```

```
[h1]Create output folder if it doesn't exist[/h1]
if (!(Test-Path $outputFolder)) { New-Item -ItemType Directory -Path $outputFolder }
```

```
[h1]Load passwords and process in parallel[/h1]
Get-Content $wordlist | ForEach-Object -Parallel {
    $password = $_
    $viewer = $using:viewerPath
    $target = $using:targetFile
    $outDir = $using:outputFolder
```

```
    # Start the process as High Priority
    $proc = Start-Process -FilePath $viewer -ArgumentList "/decrypt=""$target"",
"/pwd=""$password"" -PassThru -NoNewWindow
    $proc.PriorityClass = "High"

    # Wait for the specific attempt to finish
    $proc.WaitForExit()

    # Log Viewer.exe creates a new file (usually .html or .txt) upon success.
    # We check if a new file appeared in the directory to identify the correct password.
    $checkSuccess = Get-ChildItem $outDir | Where-Object { $_.LastWriteTime -gt
(Get-Date).AddSeconds(-5) }

    if ($checkSuccess) {
        Write-Host "[SUCCESS] Password found: $password" -ForegroundColor Green
        $password | Out-File "$outDir\FOUND_PASSWORD.txt"
        # Optional: Stop all other attempts if one succeeds
        # Get-Process "Log Viewer" | Stop-Process
    }
} -ThrottleLimit [int]$env:NUMBER_OF_PROCESSORS
```

=====

I guess our best approach is to bruteforce with list, ill try to code smthn for u to make it as fast as possible!

If the encryption algorithm is reverse-engineered, a GPU implementation could achieve 1000+ attempts/second.

omg big news im stupid. i found something so soo helpful!! i gotta finsih this all by tonight. i need u to send me the files asap, specially the log examples u have. so i can help u further. start Convo or private message me.

Hey man, you got me very excited lol. I did something similar to your powershell script but it would take days. I'd love to open up a DM but this site doesn't let me. How can we move forward?

(Dec 25, 2025 11:45 AM)qupuf Wrote: [\[CITE\]](#) Hey man, you got me very excited lol. I did something similar to your powershell script but it would take days. I'd love to open up a DM but this site doesn't let me. How can we move forward?

i sent u pm back, yea dw about the powershell stuff i was just trying to test stuff, i still have more things to test but i cooked smthn for u. check pm

dudddde hop on dm as fast as possible! i think we did it!!!! holyshit i spent lotsa hours on this :O im tired now i take break but send me message wen u see this!

qupuf - December 26, 2025, 9:31 pm

For anyone wondering, I can confirm M0HX user is 100% legit. He helped me out and actually cracked the .ple! He was very nice and didn't even ask for a tip (but I gave em).

Thank you M0HX or MOHX! <3

m0hx - December 27, 2025, 2:27 am

(Dec 26, 2025 10:31 PM)qupuf Wrote: [\[CITE\]](#) For anyone wondering, I can confirm M0HX user is 100% legit. He helped me out and actually cracked the .ple! He was very nice and didn't even ask for a tip (but I gave em).

Thank you M0HX or MOHX! <3

ayy ty for the shoutout? we cracked the code friend! without ur help i couldn't have figured it out myself. thanks for the resources :p now we can crack any file ???

InterFear - December 27, 2025, 4:36 am

(Dec 27, 2025 03:27 AM)m0hx Wrote: [\[CITE\]](#) ayy ty for the shoutout? we cracked the code friend! without ur help i couldn't have figured it out myself. thanks for the resources :p now we can crack any file ???

fair play. Good to see a real mandem