PRZYKŁADY DZIAŁANIA

Zadanie 1 i 2

Klasa SSHLogEntry oraz klasy dziedziczące

Tworzymy 4 przykładowe obiekty

```python
from zad1_6 import FailedPassword,AcceptedPassword,Error,OtherInfo


log1= FailedPassword('Dec 22 04:50:18 LabSZ sshd[22642]: Failed password for invalid user default from 46.148.21.32 port 37906 ssh2')
print(log1.turnToString())

log2= AcceptedPassword('Dec 21 23:42:08 LabSZ sshd[21010]: Accepted password for hxu from 111.222.107.90 port 43009 ssh2')
print(log2.turnToString())

log3= Error('Dec 22 04:50:19 LabSZ sshd[22647]: error: Received disconnect from 195.154.37.122: 3: com.jcraft.jsch.JSchException: Auth fail [preauth]')
print(log3.turnToString())

log4= OtherInfo('Dec 21 23:43:58 LabSZ sshd[21115]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=114.112.48.155  user=root')
print(log4.turnToString())
```

```
student@jezyki-skryptowe:~/Pulpit/Lab6$ python main.py
Dec 22 04:50:18 LabSZ sshd[22642]: Password rejected for user default from 46.148.21.32
Dec 21 23:42:08 LabSZ sshd[21010]: Password accepted for user hxu from 111.222.107.90
Dec 22 04:50:19 LabSZ sshd[22647]: IP address: 195.154.37.122, Error message: com.jcraft.jsch.JSchException: Auth fail
Dec 21 23:43:58 LabSZ sshd[21115]: Info: : pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=114.112.48.155  user=root
```

Jeżeli logi które podamy będą niewłaściwe, to dostaniemy odpowiednie komunikaty.

```python
from zad1_6 import FailedPassword,AcceptedPassword,Error,OtherInfo


log1= FailedPassword('Dec 21 23:43:58 LabSZ sshd[21115]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=114.112.48.155  user=root')
print(log1.turnToString())

log2= AcceptedPassword('Dec 21 23:43:58 LabSZ sshd[21115]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=114.112.48.155  user=root')
print(log2.turnToString())

log3= Error('Dec 21 23:43:58 LabSZ sshd[21115]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=114.112.48.155  user=root')
print(log3.turnToString())

log4= OtherInfo('Dec 21 23:42:08 LabSZ sshd[21010]: Accepted password for hxu from 111.222.107.90 port 43009 ssh2')
print(log4.turnToString())
```

```
student@jezyki-skryptowe:~/Pulpit/Lab6$ python main.py
Podany log nie jest może być obiektem FailedPassword
Brak potrzebnych parametrow
None
Podany log nie jest może być obiektem AcceptedPassword
Brak potrzebnych parametrow
None
Podany log nie jest może być obiektem Error
Brak potrzebnych parametrow
None
Podany log nie może być obiektem OtherInfo
Log powinien byc obiektem FailedPassword, AcceptedPassword lub Error
None
```

Metoda checkIfIP:

```python
from zad1_6 import FailedPassword,AcceptedPassword,Error,OtherInfo


log1= FailedPassword('Dec 22 04:50:18 LabSZ sshd[22642]: Failed password for invalid user default from 46.148.21.32 port 37906 ssh2')
print(log1.turnToString())
print(log1.checkIfIP())

log2= AcceptedPassword('Dec 21 23:42:08 LabSZ sshd[21010]: Accepted password for hxu from 111.222.107.90 port 43009 ssh2')
print(log2.turnToString())
print(log2.checkIfIP())

log3= Error('Dec 22 04:50:19 LabSZ sshd[22647]: error: Received disconnect from 195.154.37.122: 3: com.jcraft.jsch.JSchException: Auth fail [preauth]')
print(log3.turnToString())
print(log3.checkIfIP())

log4= OtherInfo('Dec 21 23:42:08 LabSZ sshd[21010]: pam_unix(sshd:session): session opened for user hxu by (uid=0)')
print(log4.turnToString())
print(log4.checkIfIP())
```

Jeżeli w logu jest adres ip to zwracamy obiekt IPv4Address, a jak nie ma - None

```
student@jezyki-skryptowe:~/Pulpit/Lab6$ python main.py
Dec 22 04:50:18 LabSZ sshd[22642]: Password rejected for user default from 46.148.21.32
Stworzono obiekt IPv4Address
<zad1_6.IPv4Address object at 0x7facd80aba60>
Dec 21 23:42:08 LabSZ sshd[21010]: Password accepted for user hxu from 111.222.107.90
Stworzono obiekt IPv4Address
<zad1_6.IPv4Address object at 0x7facd8053fa0>
Dec 22 04:50:19 LabSZ sshd[22647]: IP address: 195.154.37.122, Error message: com.jcraft.jsch.JSchException: Auth fail
Stworzono obiekt IPv4Address
<zad1_6.IPv4Address object at 0x7facd8053f70>
Dec 21 23:42:08 LabSZ sshd[21010]: Info: : pam_unix(sshd:session): session opened for user hxu by (uid=0)
None
```

Zadania 3

Funkcja validate(). weryfikuje, czy zawartość surowej treści wpisu jest zgodna z pozostałymi, wyekstrahowanymi atrybutami. Funkcja w klasie reprezentującą inną informację zawsze zwraca prawdę.

main.py > ...

```python
from zad1_6 import FailedPassword,AcceptedPassword,Error,OtherInfo


log1= FailedPassword('Dec 22 04:50:18 LabSZ sshd[22642]: Failed password for invalid user default from 46.148.21.32 port 37906 ssh2')
print(log1.turnToString())
#print(log1.checkIfIP())
print(log1.user)
print(log1.validate())
log1.user='other user'
print(log1.user)
print(log1.validate())

log2= AcceptedPassword('Dec 21 23:42:08 LabSZ sshd[21010]: Accepted password for hxu from 111.222.107.90 port 43009 ssh2')
print(log2.turnToString())
#print(log2.checkIfIP())
print(log2.validate())

log3= Error('Dec 22 04:50:19 LabSZ sshd[22647]: error: Received disconnect from 195.154.37.122: 3: com.jcraft.jsch.JSchException: Auth fail [preauth]')
print(log3.turnToString())
#print(log3.checkIfIP())
print(log3.validate())

log4= OtherInfo('Dec 21 23:42:08 LabSZ sshd[21010]: pam_unix(sshd:session): session opened for user hxu by (uid=0)')
print(log4.turnToString())
#print(log4.checkIfIP())
print(log4.time)
print(log4.validate())
log4.host='other time'
print(log4.time)
print(log4.validate())
```

Gdy zmienimy usera z ‘default’ na ‘other user’ otrzymujemy False:

```
student@jezyki-skryptowe:~/Pulpit/Lab6$ python main.py
Dec 22 04:50:18 LabSZ sshd[22642]: Password rejected for user default from 46.148.21.32
default
True
other user
False
Dec 21 23:42:08 LabSZ sshd[21010]: Password accepted for user hxu from 111.222.107.90
True
Dec 22 04:50:19 LabSZ sshd[22647]: IP address: 195.154.37.122, Error message: com.jcraft.jsch.JSchException: Auth fail
True
Dec 21 23:42:08 LabSZ sshd[21010]: Info: : pam_unix(sshd:session): session opened for user hxu by (uid=0)
LabSZ
True
other host
True
```

Zadanie 4

W klasie SSHLogEntry, określ atrybut reprezentujący surową treść wpisu jako część niepublicznego API.

```python
class SSHLogEntry(metaclass=abc.ABCMeta):
    def __init__(self, log_line):
        self.time = None
        self.host = None
        self._raw_text = log_line
        self.pid = None
```

Zadanie 5

W klasie SSHLogEntry, zdefiniować właściwość (property) tylko do odczytu o nazwie has_ip, która będzie miała wartość True, gdy we wpisie występuje adres IP, w przeciwnym wypadku False.

```python
from zad1_6 import FailedPassword,AcceptedPassword,Error,OtherInfo


log1= FailedPassword('Dec 22 04:50:18 LabSZ sshd[22642]: Failed password for invalid user default from 46.148.21.32 port 37906 ssh2')
print(log1.turnToString())
#print(log1.checkIfIP())
#print(log1.user)
#print(log1.validate())
#log1.user='other user'
#print(log1.user)
#print(log1.validate())
print(log1.has_ip)

log2= AcceptedPassword('Dec 21 23:42:08 LabSZ sshd[21010]: Accepted password for hxu from 111.222.107.90 port 43009 ssh2')
print(log2.turnToString())
#print(log2.checkIfIP())
#print(log2.validate())
print(log2.has_ip)

log3= Error('Dec 22 04:50:19 LabSZ sshd[22647]: error: Received disconnect from 195.154.37.122: 3: com.jcraft.jsch.JSchException: Auth fail [preauth]')
print(log3.turnToString())
#print(log3.checkIfIP())
#print(log3.validate())
print(log3.has_ip)

log4= OtherInfo('Dec 21 23:42:08 LabSZ sshd[21010]: pam_unix(sshd:session): session opened for user hxu by (uid=0)')
print(log4.turnToString())
#print(log4.checkIfIP())
#print(log4.time)
#print(log4.validate())
#log4.host='other time'
#print(log4.time)
#print(log4.validate())
print(log4.has_ip)
```

```
student@jezyki-skryptowe:~/Pulpit/Lab6$ python main.py
Dec 22 04:50:18 LabSZ sshd[22642]: Password rejected for user default from 46.148.21.32
Stworzono obiekt IPv4Address
True
Dec 21 23:42:08 LabSZ sshd[21010]: Password accepted for user hxu from 111.222.107.90
Stworzono obiekt IPv4Address
True
Dec 22 04:50:19 LabSZ sshd[22647]: IP address: 195.154.37.122, Error message: com.jcraft.jsch.JSchException: Auth fail
Stworzono obiekt IPv4Address
True
Dec 21 23:42:08 LabSZ sshd[21010]: Info: : pam_unix(sshd:session): session opened for user hxu by (uid=0)
False
```

Zadanie 6

W klasie SSHLogEntry zaproponować implementacje metod magicznych __repr__, __eq__, __lt__, __gt__.

Testujemy dla tych samych logów co wcześniej:

```python
print(log1)
print(log2)
print(log3)
print(log2 < log1)
print(log2 > log1)
print(log1==log3)
print(log1 == log1)

```

```
student@jezyki-skryptowe:~/Pulpit/Lab6$ python main.py
Time: Dec 22 04:50:18, Host: LabSZ, PID: sshd[22642], Raw_text: Dec 22 04:50:18 LabSZ sshd[22642]: Failed password for invalid
user default from 46.148.21.32 port 37906 ssh2
Time: Dec 21 23:42:08, Host: LabSZ, PID: sshd[21010], Raw_text: Dec 21 23:42:08 LabSZ sshd[21010]: Accepted password for hxu fr
om 111.222.107.90 port 43009 ssh2
Time: Dec 22 04:50:19, Host: LabSZ, PID: sshd[22647], Raw_text: Dec 22 04:50:19 LabSZ sshd[22647]: error: Received disconnect f
rom 195.154.37.122: 3: com.jcraft.jsch.JSchException: Auth fail [preauth]
True
False
False
True
```

Logi nie są wyswietlone ładnie po jednym w każdej linijce, bo musiałam zwężyć terminal, żeby cokolwiek było potem widoczne w dokumencie.

Zadanie 7

Klasa SSHLogJournal i metoda pozwalającą pobrać fragment listę logów wg. wybranego samodzielnie kryterium

```
47
48  journal = SSHLogJournal()
49
50  journal.append('Dec 21 23:48:15 LabSZ sshd[21169]: Invalid user test2 from 122.224.69.34')
51  journal.append('Dec 21 23:45:35 LabSZ sshd[21165]: Failed password for root from 114.112.48.155 port 46140 ssh2')
52  journal.append('Dec 21 23:42:08 LabSZ sshd[21010]: Accepted password for hxu from 111.222.107.90 port 43009 ssh2')
53  print(journal.logs)
54
55  print(journal.get_logs_by_criteria(lambda x: True if (x.ip=='114.112.48.155') else False))
56  print(journal.get_logs_by_criteria(lambda x: True if (x.ip=='random ip') else False))
57
```

```
student@jezyki-skryptowe:~/Pulpit/Lab6$ python zad7.py
[Time: Dec 21 23:48:15, Host: LabSZ, PID: sshd[21169], Raw_text: Dec 21 23:48:15 LabSZ sshd[21169]: Invalid user test2 from 122.224.69.34, Time: D
ec 21 23:45:35, Host: LabSZ, PID: sshd[21165], Raw_text: Dec 21 23:45:35 LabSZ sshd[21165]: Failed password for root from 114.112.48.155 port 4614
0 ssh2, Time: Dec 21 23:42:08, Host: LabSZ, PID: sshd[21010], Raw_text: Dec 21 23:42:08 LabSZ sshd[21010]: Accepted password for hxu from 111.222.
107.90 port 43009 ssh2]
[Time: Dec 21 23:45:35, Host: LabSZ, PID: sshd[21165], Raw_text: Dec 21 23:45:35 LabSZ sshd[21165]: Failed password for root from 114.112.48.155 p
ort 46140 ssh2]
[]
```

Zadanie 8

Kacze typowanie: klasa SSHUser reprezentująca użytkownika

```
17  log_journal = SSHLogJournal()
18  log_journal.append('Dec 21 23:43:52 LabSZ sshd[21111]: Failed password for root from 114.112.48.155 port 56398 ssh2')
19  log_journal.append('Dec 21 23:43:52 LabSZ sshd[21111]: Received disconnect from 114.112.48.155: 11: Bye Bye [preauth]')
20  log_journal.append('Dec 21 23:43:53 LabSZ sshd[21113]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=114.112.48.155  user=root')
21  log_journal.append('Dec 21 23:43:55 LabSZ sshd[21113]: Failed password for root from 114.112.48.155 port 58287 ssh2')
22  log_journal.append('Dec 21 23:43:56 LabSZ sshd[21113]: Received disconnect from 114.112.48.155: 11: Bye Bye [preauth]')
23
24  user1 = SSHUser("admin",'Dec 21 23:43:52')
25  user2 = SSHUser("uzytkownik",'Dec 22 23:53:52')
26
27  final_lst = []
28  for log in log_journal:
29      final_lst.append(log)
30  #print(final_lst)
31
32  final_lst.append(user1)
33  final_lst.append(user2)
34  print(final_lst)
35
36  for log in final_lst:
37      print(log.validate())
38      print("Zwalidowano")
```

Do final_lst z powodzeniem dodajemy zarówno obiekty SSHLogJournal jak i obiekty SSHUser i następnie iterujemy po całej liście wykonując metodę validate().

```
student@jezyki-skryptowe:~/Pulpit/Lab6$ python zad8.py
[Time: Dec 21 23:43:52, Host: LabSZ, PID: sshd[21111], Raw_text: Dec 21 23:43:52 LabSZ sshd[21111]: Failed password for root from 114.112.48.155 port 56398 ssh2, Time:
Dec 21 23:43:52, Host: LabSZ, PID: sshd[21111], Raw_text: Dec 21 23:43:52 LabSZ sshd[21111]: Received disconnect from 114.112.48.155: 11: Bye Bye [preauth], Time: Dec 2
1 23:43:53, Host: LabSZ, PID: sshd[21113], Raw_text: Dec 21 23:43:53 LabSZ sshd[21113]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser
= rhost=114.112.48.155  user=root, Time: Dec 21 23:43:55, Host: LabSZ, PID: sshd[21113], Raw_text: Dec 21 23:43:55 LabSZ sshd[21113]: Failed password for root from 114.
112.48.155 port 58287 ssh2, Time: Dec 21 23:43:56, Host: LabSZ, PID: sshd[21113], Raw_text: Dec 21 23:43:56 LabSZ sshd[21113]: Received disconnect from 114.112.48.155:
11: Bye Bye [preauth], <__main__.SSHUser object at 0x7fda7c30dae0>, <__main__.SSHUser object at 0x7fda7c30d720>]
True
Zwalidowano
True
Zwalidowano
True
Zwalidowano
True
Zwalidowano
True
Zwalidowano
True
Zwalidowano
True
Zwalidowano
```