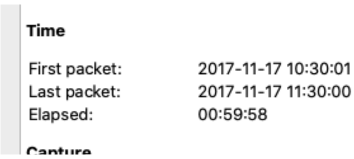
Answers: Using Wireshark

1) Which day this capture was realized?



Time

First packet:	2017-11-17 10:30:01
Last packet:	2017-11-17 11:30:00
Elapsed:	00:59:58

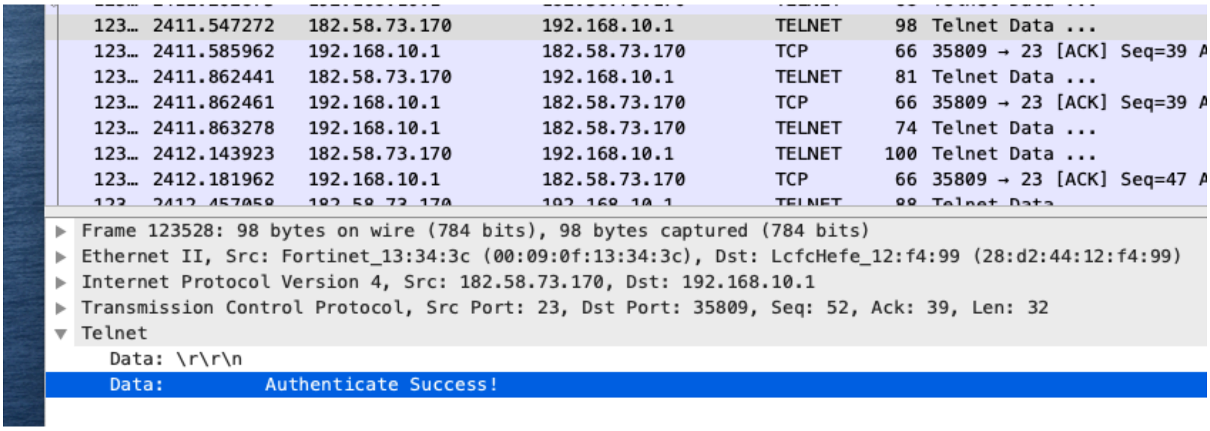
Capture

2) Which PROTOCOL did Malware use to test Users/Passwords?

R: TELNET/23

3) Identify the compromised device (IP ADRESS).

R: 192.168.10.1

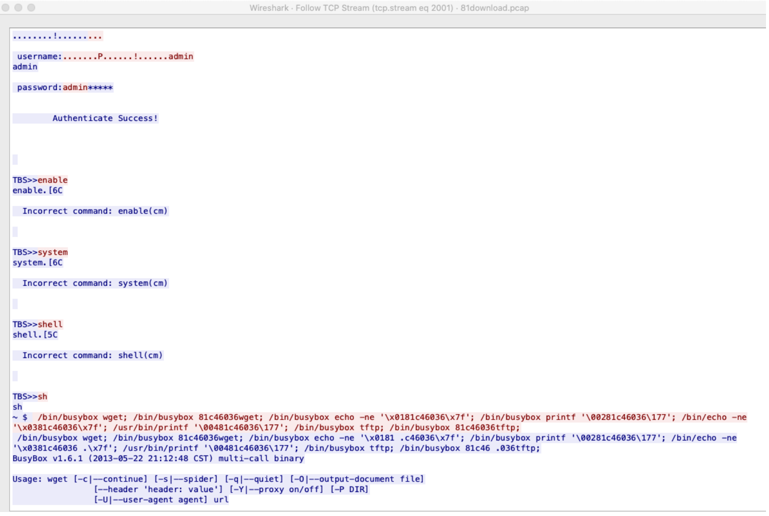


```
123…  2411.547272  182.58.73.170  192.168.10.1   TELNET   98 Telnet Data ...
123…  2411.585962  192.168.10.1   182.58.73.170  TCP      66 35809 → 23 [ACK] Seq=39 A
123…  2411.862441  182.58.73.170  192.168.10.1   TELNET   81 Telnet Data ...
123…  2411.862461  192.168.10.1   182.58.73.170  TCP      66 35809 → 23 [ACK] Seq=39 A
123…  2411.863278  192.168.10.1   182.58.73.170  TELNET   74 Telnet Data ...
123…  2412.143923  182.58.73.170  192.168.10.1   TELNET  100 Telnet Data ...
123…  2412.181962  192.168.10.1   182.58.73.170  TCP      66 35809 → 23 [ACK] Seq=47 A
123…  2412.457058  182.58.73.170  192.168.10.1   TELNET   98 Telnet Data ...
```

```
▶ Frame 123528: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: Fortinet_13:34:3c (00:09:0f:13:34:3c), Dst: LcfcHefe_12:f4:99 (28:d2:44:12:f4:99)
▶ Internet Protocol Version 4, Src: 182.58.73.170, Dst: 192.168.10.1
▶ Transmission Control Protocol, Src Port: 23, Dst Port: 35809, Seq: 52, Ack: 39, Len: 32
▼ Telnet
    Data: \r\r\n
    Data:         Authenticate Success!
```

4) What was the USER/PASSWORD used to get access? (print the result of "follow TCP stream") showing the pair user/password.

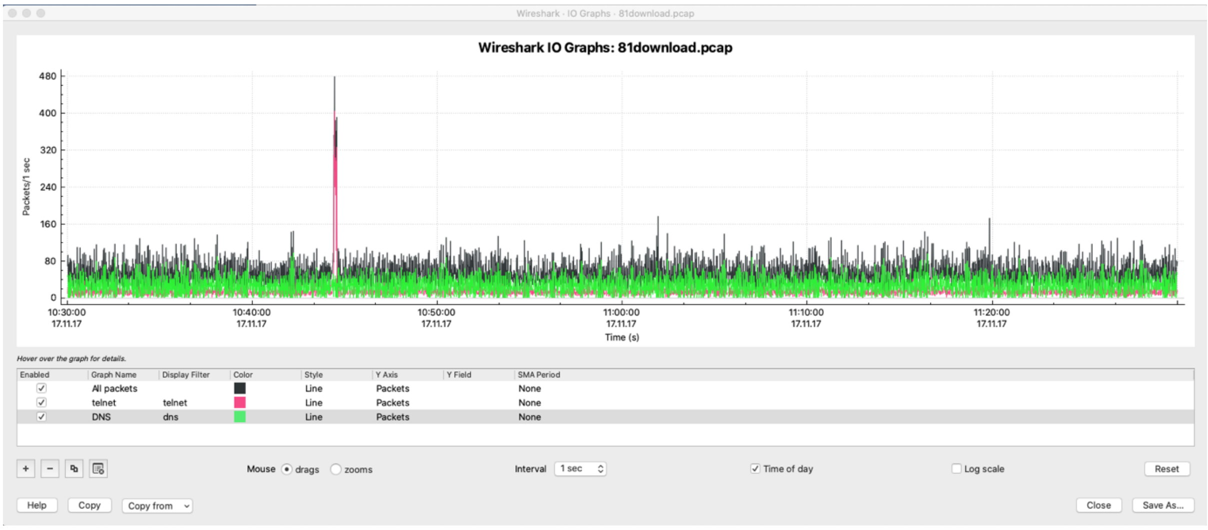
R: admin/admin



Wireshark · Follow TCP Stream (tcp.stream eq 2001) · 81download.pcap

```
........!.........

 username:.......P......!......admin
admin

 password:admin*****


        Authenticate Success!




TBS>>enable
enable.[6C

  Incorrect command: enable(cm)



TBS>>system
system.[6C

  Incorrect command: system(cm)



TBS>>shell
shell.[5C

  Incorrect command: shell(cm)



TBS>>sh
sh
~ $  /bin/busybox wget; /bin/busybox 81c46036wget; /bin/busybox echo -ne '\x0181c46036\x7f'; /bin/busybox printf '\00281c46036\177'; /bin/echo -ne
'\x0381c46036\x7f'; /usr/bin/printf '\00481c46036\177'; /bin/busybox tftp; /bin/busybox 81c46036tftp;
 /bin/busybox wget; /bin/busybox 81c46036wget; /bin/busybox echo -ne '\x0181 .c46036\x7f'; /bin/busybox printf '\00281c46036\177'; /bin/echo -ne
'\x0381c46036 .\x7f'; /usr/bin/printf '\00481c46036\177'; /bin/busybox tftp; /bin/busybox 81c46 .036tftp;
BusyBox v1.6.1 (2013-05-22 21:12:48 CST) multi-call binary

Usage: wget [-c|--continue] [-s|--spider] [-q|--quiet] [-O|--output-document file]
                [--header 'header: value'] [-Y|--proxy on/off] [-P DIR]
                [-U|--user-agent agent] url
```

5) Use the menu “Statistics → IO Graph” to generate a graph including all of these items:



Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	All packets		⬛	Line	Packets		None
☑	telnet	telnet	🟥	Line	Packets		None
☑	DNS	dns	🟩	Line	Packets		None

Mouse ● drags ○ zooms

Interval 1 sec

☑ Time of day

□ Log scale