

Lab 7

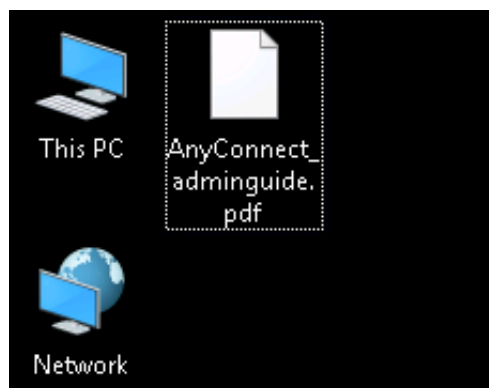
Authors: Daniel Gisolfi, James Ekstract

Section 1

Screen capture showing the alert script within the tcpdumpcapturefile file

```
15:52:38.175584 IP 172.30.0.2.49709 > 172.30.0.13.80: Flags [P.], seq 1:504, ack 1, win 32768, length 503: HTTP: GET /DVWA/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%27this+is+a+vulnerability%27%29%3B%3C%2Fscript%3E HTTP/1.1
```

Screen capture showing the AnyConnect_adminguide.pdf on the TargetWindows02 desktop



Screen capture showing the Protocol Hierarchy Statistics

Screen capture showing the Packet Lengths distribution

Wireshark · Packet Lengths · wireshark_414269F4-8DF0-4852-8F56-384E405060F3_20200329164252_a01956

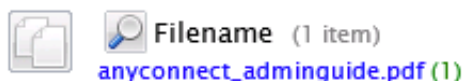
Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ Packet Lengths	21051	386.65	54	1514	0.0621	100%	20.6700	20.982
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	10056	59.69	54	73	0.0297	47.77%	6.6100	330.720
80-159	58	93.12	85	138	0.0002	0.28%	0.1000	230.674
160-319	7	241.29	176	294	0.0000	0.03%	0.0300	0.000
320-639	9427	558.00	558	558	0.0278	44.78%	6.6100	330.720
640-1279	6	882.67	858	1006	0.0000	0.03%	0.0600	20.995
1280-2559	1497	1514.00	1514	1514	0.0044	7.11%	14.9700	20.984
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Display filter: Apply

Copy Save as... Close

Screen capture showing the password and filename used in the FTP transfer

Screen capture showing the filename used in the TFTP file transfer and paste it into your Lab Report file.



Section 2

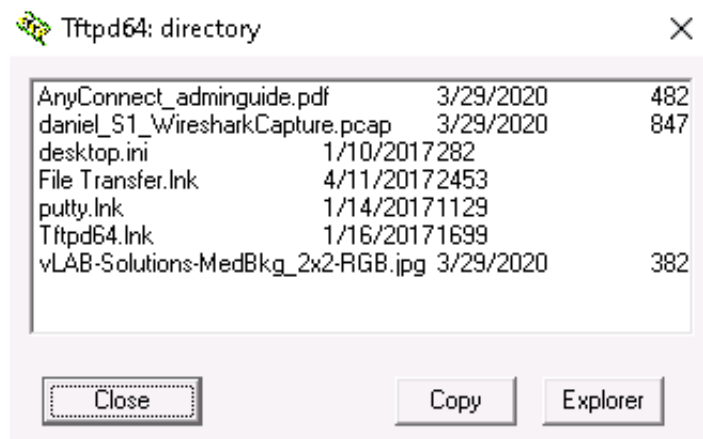
Screen capture showing the alert script in the tcpdumpcapturefile_S2 file

```
172.30.0.13 - PuTTY
root@dvwa:~# tcpdump -n -r tcpdumpcapturefile_S2 | grep alert
reading from file tcpdumpcapturefile_S2, link-type EN10MB (Ethernet)
17:38:18.014323 IP 172.30.0.2.49766 > 172.30.0.13.80: Flags [P.], seq 1:512, ack
1, win 32768, length 511: HTTP: GET /DVWA/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%27It+is+time+to+renew+your+order%27%29%3B%3C%2Fscript%3E HTTP/1.1
root@dvwa:~#
```

Screen capture showing the vLAB-Solutions-MedBkg_2x2-RGB.jpg on the TargetWindows02 desktop

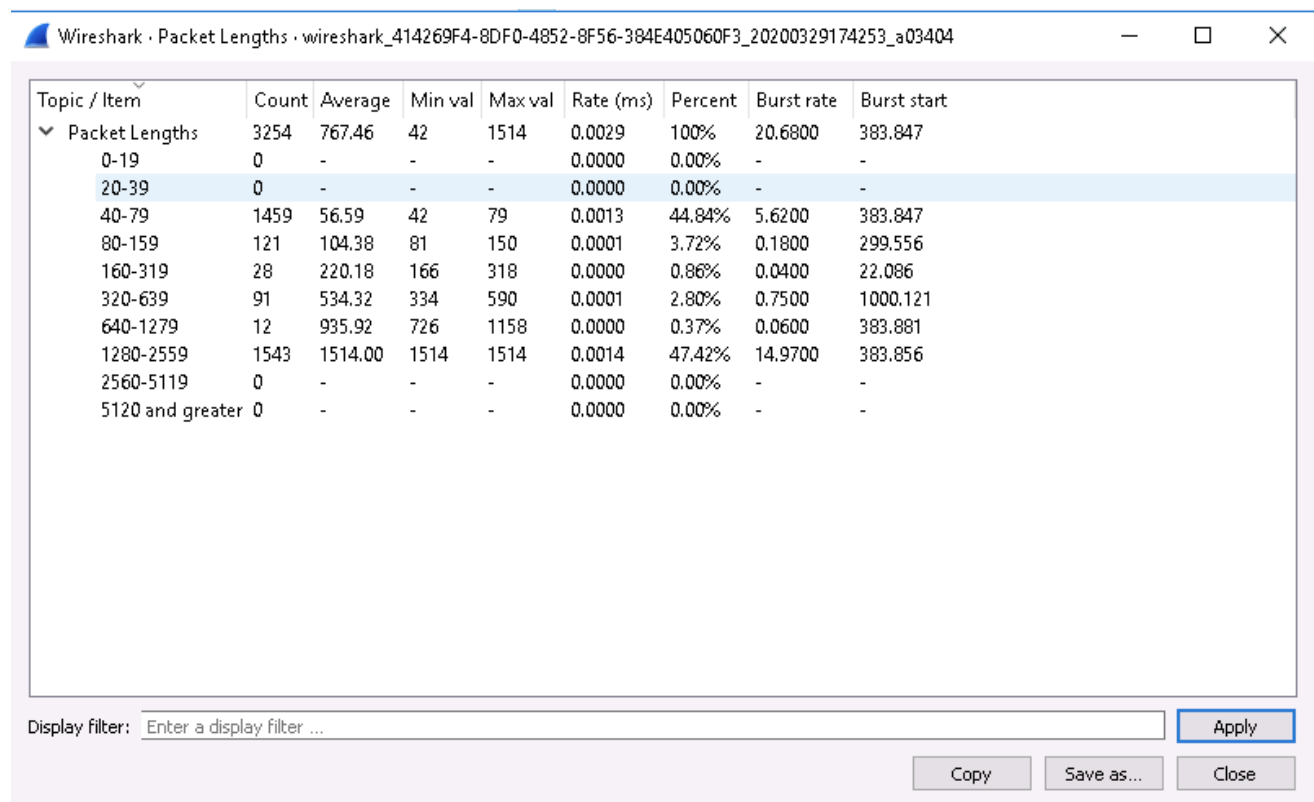


Screen capture showing the transferred file in the Tftpd64:directory window



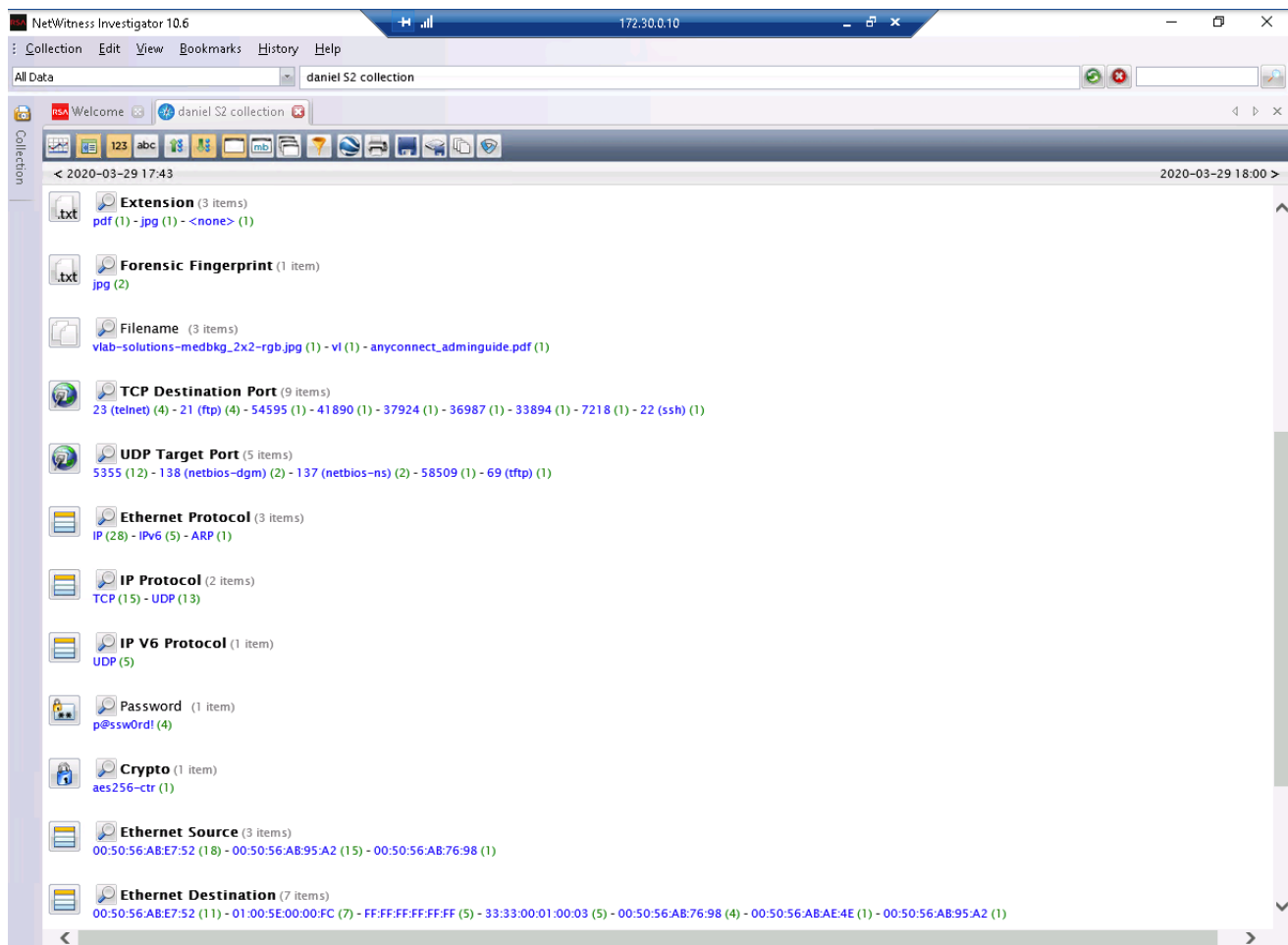
Screen capture showing the Protocol Hierarchy Statistics a

Screen capture showing the Packet Lengths distribution

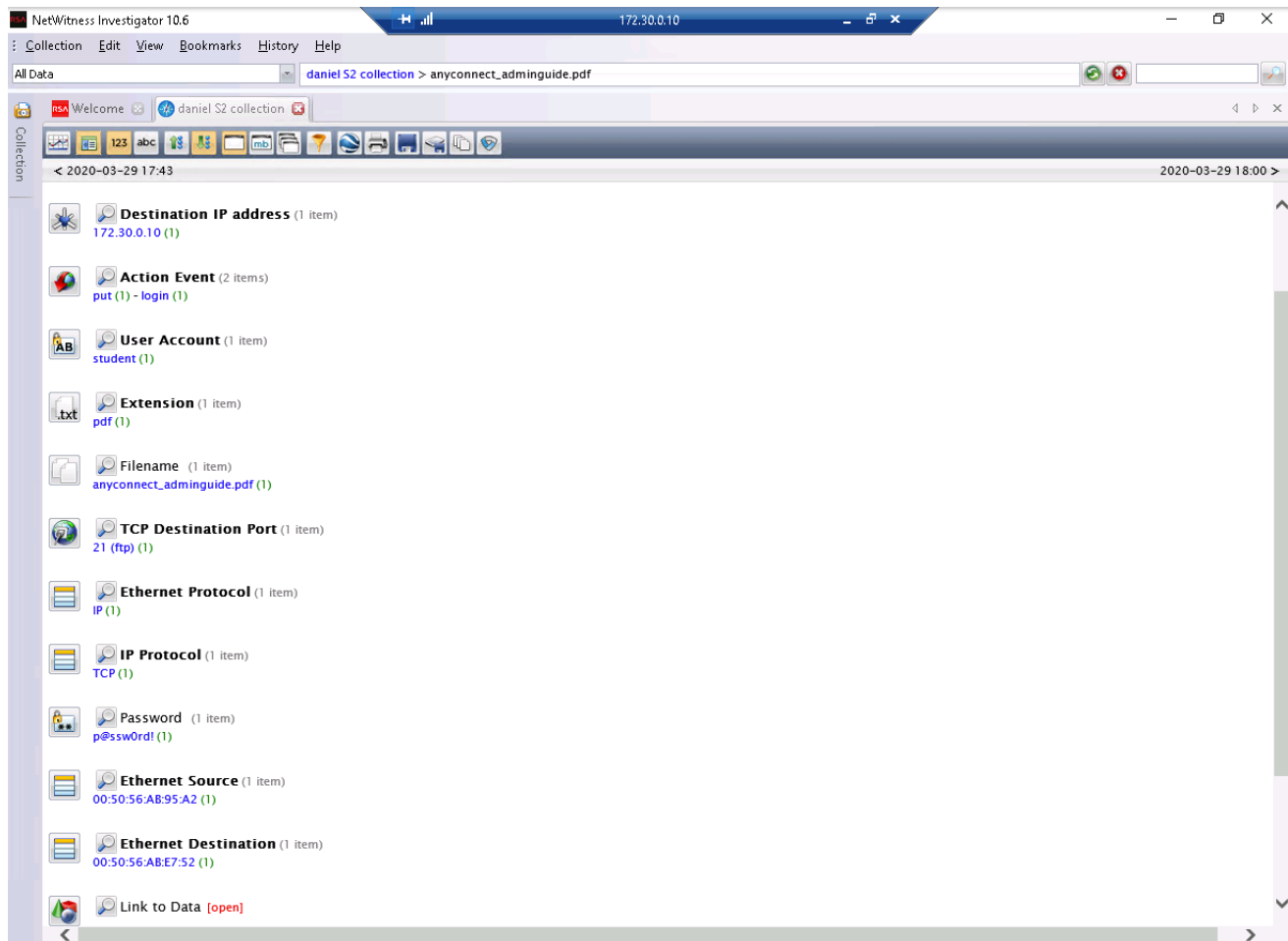


Screen capture showing the Capture File Properties

Screen capture showing the password and filename used in the FTP transfer



Screen capture showing the filename used in the TFTP file transfer



Screen capture showing the IP addresses for the SSH sessions



Screen capture showing the two column cisco packet stream

