

## Q. How to get TCP/IP communication log?

**A: Follow the procedure described below:**

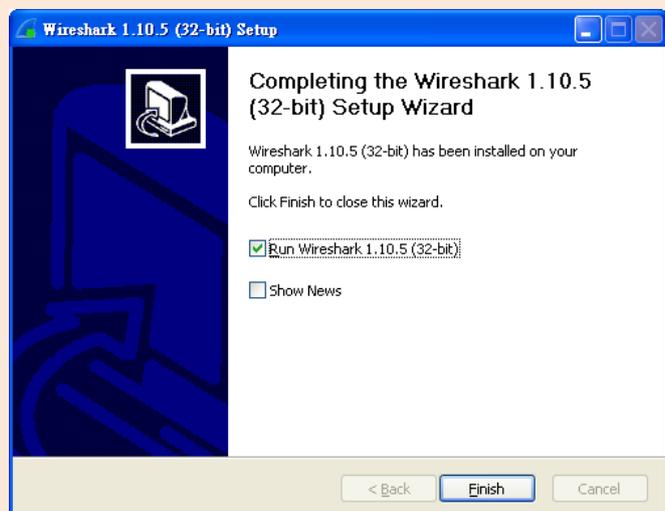
**Step 1:** Download the **Wireshark** utility, the **Wireshark** is a free and open-source packet analyzer. You can get it from the following web:  
<http://www.wireshark.org/download.html>



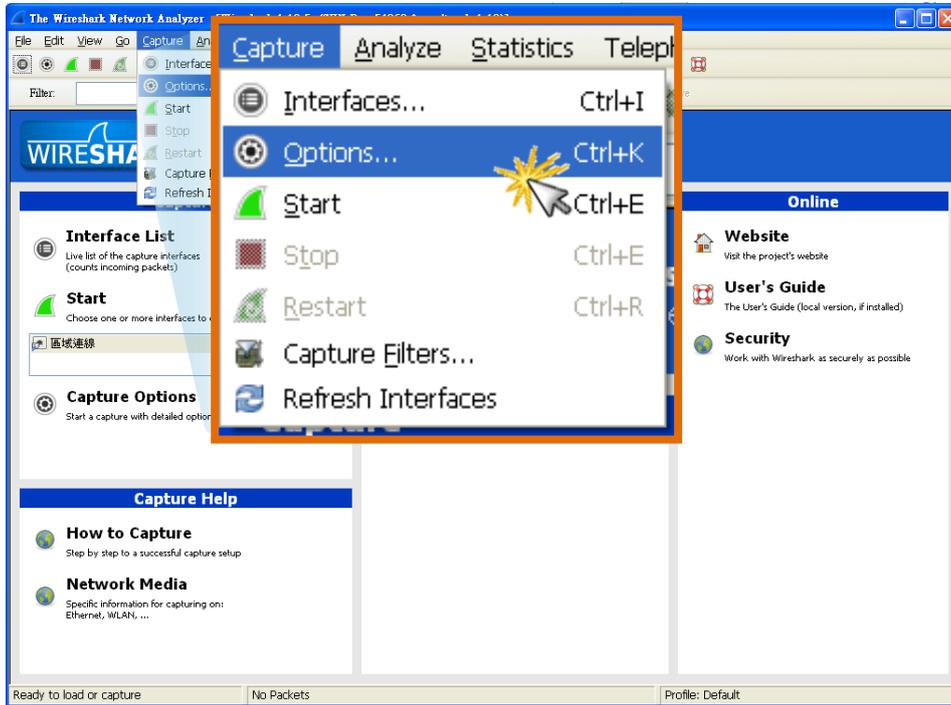
**Step 2:** Double click Wireshark setup file to install the Wireshark utility on your PC. Please follow these steps: (for example, install Wireshark under 32-bit Windows XP)

1. Click the **"Next>"** button to start the **Wireshark** installation.
2. Click the **"I Agree>"** button to continue on the **"License Agreement"** window.
3. Click the **"Next>"** button to continue on the **"Choose components"** window.
4. Click the **"Next>"** button to continue on the **"Select Additional Tasks"** window.
5. Click the **"Next>"** button to install the driver into the **default** folder on the **"Choose Install Location"** window.
6. Click the **"Install"** button to install the **WinPcap** on the **"Install WinPacap?"** window.
7. Click the **"Next>"** button to start the **WinPcap** installation.
8. Click the **"I Agree>"** button to continue on the **"License Agreement"** window.
9. Click the **"Install"** button to install the driver on the **"Installation options"** window.
10. Click the **"Finish"** button to complete the **WinPcap** installation.
11. Come back **Wireshark** installation, click the **"Next>"** button on the **"Installation Complete"** window.
12. Check the **"Run Wireshark x.xx.x (32-bti)"** item then click the **"Finish"** button to complete the **Wireshark** installation.

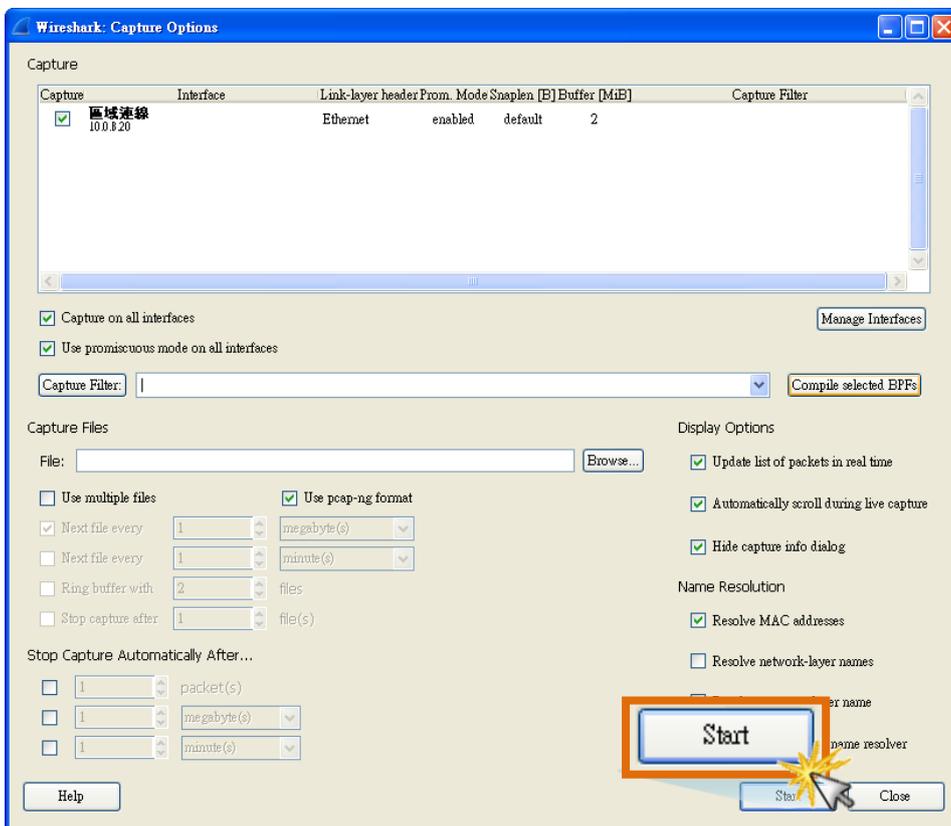
✂ For detailed information about the **Wireshark** installation, please refer to [http://www.wireshark.org/docs/wsug\\_html\\_chunked/ChBuildInstallWinInstall.html](http://www.wireshark.org/docs/wsug_html_chunked/ChBuildInstallWinInstall.html).



**Step 3:** In the WireShark utility, select the “Options...” item from the “Capture” menu.



**Step 4:** In the WireShark: Capture Options window, click “Start” button to capture TCP/IP packet.



## Step 5: Running live capture of TCP/IP communication data.

Wireshark 1.10.5 (SYN Rev 54262 from /trunk-1.10)

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
835	27.0603700	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1196 Ack=2070 win=5840 Len=3
836	27.0604210	10.0.8.20	10.0.8.11	TCP	61	4748 > ndmp [PSH, ACK] Seq=2070 Ack=1199 win=65506 Len=
837	27.0618760	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1199 Ack=2077 win=5840 Len=3
838	27.0619700	10.0.8.20	10.0.8.11	TCP	60	4748 > ndmp [PSH, ACK] Seq=2077 Ack=1202 win=65503 Len=
839	27.0634000	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1202 Ack=2083 win=5840 Len=4
840	27.0634780	10.0.8.20	10.0.8.11	TCP	58	4748 > ndmp [PSH, ACK] Seq=2083 Ack=1206 win=65499 Len=
841	27.0649060	10.0.8.11	10.0.8.20	TCP	61	ndmp > 4748 [PSH, ACK] Seq=1206 Ack=2087 win=5840 Len=7
842	27.0650330	10.0.8.20	10.0.8.11	TCP	60	4748 > ndmp [PSH, ACK] Seq=2087 Ack=1213 win=65492 Len=
843	27.0664010	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1213 Ack=2093 win=5840 Len=3
844	27.0664900	10.0.8.20	10.0.8.11	TCP	60	4748 > ndmp [PSH, ACK] Seq=2093 Ack=1216 win=65489 Len=
845	27.0678740	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1216 Ack=2099 win=5840 Len=3
846	27.1658610	10.0.8.20	10.0.8.11	TCP	54	profilemac > documentum-s [ACK] Seq=20481 Ack=21505 Win
847	27.1679910	10.0.8.20	10.0.8.11	TCP	1078	profilemac > documentum-s [PSH, ACK] Seq=20481 Ack=21505 Win
848	27.2185730	10.0.8.11	10.0.8.20	TCP	60	documentum-s > profilemac [ACK] Seq=21505 Ack=21505 Win
849	27.2664430	10.0.8.20	10.0.8.11	TCP	54	4748 > ndmp [ACK] Seq=2099 Ack=1219 win=65486 Len=0
850	27.7063040	10.0.8.11	10.0.8.20	TCP	1078	emcrrmircdd > ssad [PSH, ACK] Seq=21505 Ack=21505 Win=58
851	27.7071560	10.0.8.20	10.0.8.11	TCP	60	4748 > ndmp [PSH, ACK] Seq=2099 Ack=1219 win=65486 Len=
852	27.7086220	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1219 Ack=2105 win=5840 Len=3
853	27.7087350	10.0.8.20	10.0.8.11	TCP	60	4748 > ndmp [PSH, ACK] Seq=2105 Ack=1222 win=65483 Len=
854	27.7100950	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1222 Ack=2111 win=5840 Len=3
855	27.8105900	10.0.8.20	10.0.8.11	TCP	1078	ssad > emcrrmircdd [PSH, ACK] Seq=21505 Ack=22529 Win=65
856	27.8621040	10.0.8.11	10.0.8.20	TCP	60	emcrrmircdd > ssad [ACK] Seq=22529 Ack=22529 Win=5840 Le
857	27.8699200	10.0.8.20	10.0.8.11	TCP	54	4748 > ndmp [ACK] Seq=2111 Ack=1225 win=65480 Len=0

Frame 1: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits) on interface 0  
 Ethernet II, Src: Icpdas\_50:08:c6 (00:0d:e0:50:08:c6), Dst: AsustekCa:28:c9 (74:d0:2b:ca:28:c9)  
 Internet Protocol Version 4, Src: 10.0.8.11 (10.0.8.11), Dst: 10.0.8.20 (10.0.8.20)  
 Transmission Control Protocol, Src Port: emcrrmircdd (10004), Dst Port: ssad (4750), Seq: 1, Ack: 1, Len: 1024  
 Data (1024 bytes)

0000 74 d0 2b ca 28 c9 00 0d e0 50 08 c6 08 00 45 00 t.+.(...P....E.  
 0010 04 28 4e cf 00 00 40 06 03 e3 0a 00 08 0b 0a 00 .(N...@.....  
 0020 08 14 27 14 12 8e 00 76 67 e5 de f2 45 03 50 18 .....v g...E.P.  
 0030 16 d0 be 35 00 00 30 30 30 30 35 35 39 3a 00 ...5...000559:.  
 0040 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 .....!.....  
 0050 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 .....!##%&'()\*  
 0060 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 \*+,-./0123456789  
 0070 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 ;<=>?@A BCDEFGHI  
 0080 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 JKL MNOPQ RSTUVWXY  
 0090 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 Z[\]^\_`abcde fghijklmno pqrstu vwxyz

## Step 6: Click the "Stop" button to stop the running live capture.

Wireshark 1.10.5 (SYN Rev 54262 from /trunk-1.10)

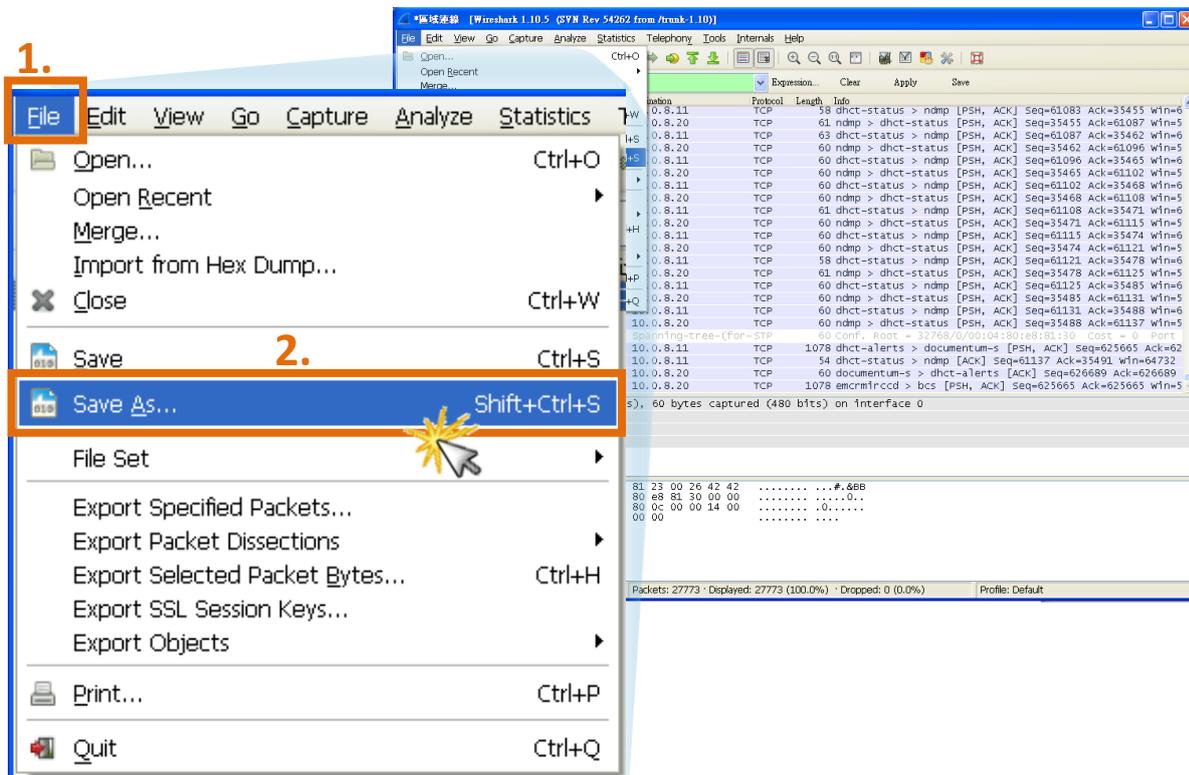
Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
835	27.0603700	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1196 Ack=2070 win=5840 Len=3
836	27.0604210	10.0.8.20	10.0.8.11	TCP	61	4748 > ndmp [PSH, ACK] Seq=2070 Ack=1199 win=65506 Len=
837	27.0618760	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1199 Ack=2077 win=5840 Len=3
838	27.0619700	10.0.8.20	10.0.8.11	TCP	60	4748 > ndmp [PSH, ACK] Seq=2077 Ack=1202 win=65503 Len=
839	27.0634000	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1202 Ack=2083 win=5840 Len=4
840	27.0634780	10.0.8.20	10.0.8.11	TCP	58	4748 > ndmp [PSH, ACK] Seq=2083 Ack=1206 win=65499 Len=
841	27.0649060	10.0.8.11	10.0.8.20	TCP	61	ndmp > 4748 [PSH, ACK] Seq=1206 Ack=2087 win=5840 Len=7
842	27.0650330	10.0.8.20	10.0.8.11	TCP	60	4748 > ndmp [PSH, ACK] Seq=2087 Ack=1213 win=65492 Len=
843	27.0664010	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1213 Ack=2093 win=5840 Len=3
844	27.0664900	10.0.8.20	10.0.8.11	TCP	60	4748 > ndmp [PSH, ACK] Seq=2093 Ack=1216 win=65489 Len=
845	27.0678740	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1216 Ack=2099 win=5840 Len=3
846	27.1658610	10.0.8.20	10.0.8.11	TCP	54	profilemac > documentum-s [ACK] Seq=20481 Ack=21505 Win
847	27.1679910	10.0.8.20	10.0.8.11	TCP	1078	profilemac > documentum-s [PSH, ACK] Seq=20481 Ack=21505 Win
848	27.2185730	10.0.8.11	10.0.8.20	TCP	60	documentum-s > profilemac [ACK] Seq=21505 Ack=21505 Win
849	27.2664430	10.0.8.20	10.0.8.11	TCP	54	4748 > ndmp [ACK] Seq=2099 Ack=1219 win=65486 Len=0
850	27.7063040	10.0.8.11	10.0.8.20	TCP	1078	emcrrmircdd > ssad [PSH, ACK] Seq=21505 Ack=21505 Win=58
851	27.7071560	10.0.8.20	10.0.8.11	TCP	60	4748 > ndmp [PSH, ACK] Seq=2099 Ack=1219 win=65486 Len=
852	27.7086220	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1219 Ack=2105 win=5840 Len=3
853	27.7087350	10.0.8.20	10.0.8.11	TCP	60	4748 > ndmp [PSH, ACK] Seq=2105 Ack=1222 win=65483 Len=
854	27.7100950	10.0.8.11	10.0.8.20	TCP	60	ndmp > 4748 [PSH, ACK] Seq=1222 Ack=2111 win=5840 Len=3
855	27.8105900	10.0.8.20	10.0.8.11	TCP	1078	ssad > emcrrmircdd [PSH, ACK] Seq=21505 Ack=22529 Win=65
856	27.8621040	10.0.8.11	10.0.8.20	TCP	60	emcrrmircdd > ssad [ACK] Seq=22529 Ack=22529 Win=5840 Le
857	27.8699200	10.0.8.20	10.0.8.11	TCP	54	4748 > ndmp [ACK] Seq=2111 Ack=1225 win=65480 Len=0

Frame 1: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits) on interface 0  
 Ethernet II, Src: Icpdas\_50:08:c6 (00:0d:e0:50:08:c6), Dst: AsustekCa:28:c9 (74:d0:2b:ca:28:c9)  
 Internet Protocol Version 4, Src: 10.0.8.11 (10.0.8.11), Dst: 10.0.8.20 (10.0.8.20)  
 Transmission Control Protocol, Src Port: emcrrmircdd (10004), Dst Port: ssad (4750), Seq: 1, Ack: 1, Len: 1024  
 Data (1024 bytes)

0000 74 d0 2b ca 28 c9 00 0d e0 50 08 c6 08 00 45 00 t.+.(...P....E.  
 0010 04 28 4e cf 00 00 40 06 03 e3 0a 00 08 0b 0a 00 .(N...@.....  
 0020 08 14 27 14 12 8e 00 76 67 e5 de f2 45 03 50 18 .....v g...E.P.  
 0030 16 d0 be 35 00 00 30 30 30 30 35 35 39 3a 00 ...5...000559:.  
 0040 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 .....!.....  
 0050 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 .....!##%&'()\*  
 0060 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 \*+,-./0123456789  
 0070 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 ;<=>?@A BCDEFGHI  
 0080 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 JKL MNOPQ RSTUVWXY  
 0090 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 Z[\]^\_`abcde fghijklmno pqrstu vwxyz

**Step 7:** Select the “Save As...” item from the “File” menu to save captured packets.

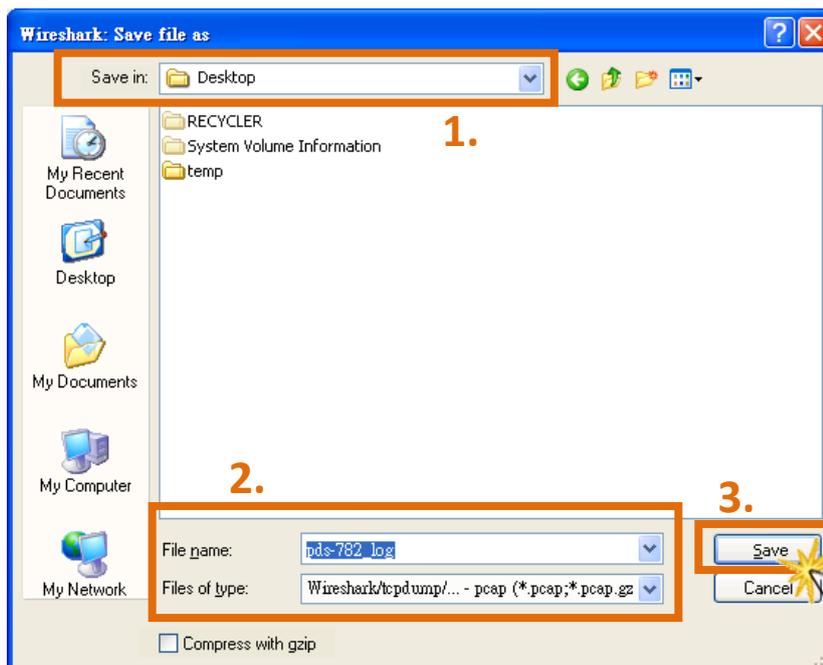


**Step 8:** In the “Wireshark: Save file as” dialog box, select destination folder to saved capture file.

**Step 9:** Type file name in the **File Name:** field (for example, pds-782\_log).

**Step 10:** Specify the **default file save format (\*.pcap)** of the **WireShark** by clicking on the **Files of type:** type drop down box.

**Step 11:** Click “Save” button.



**(Finish)**