

\*\*\*\*\*Draft\*\*\*\*\*

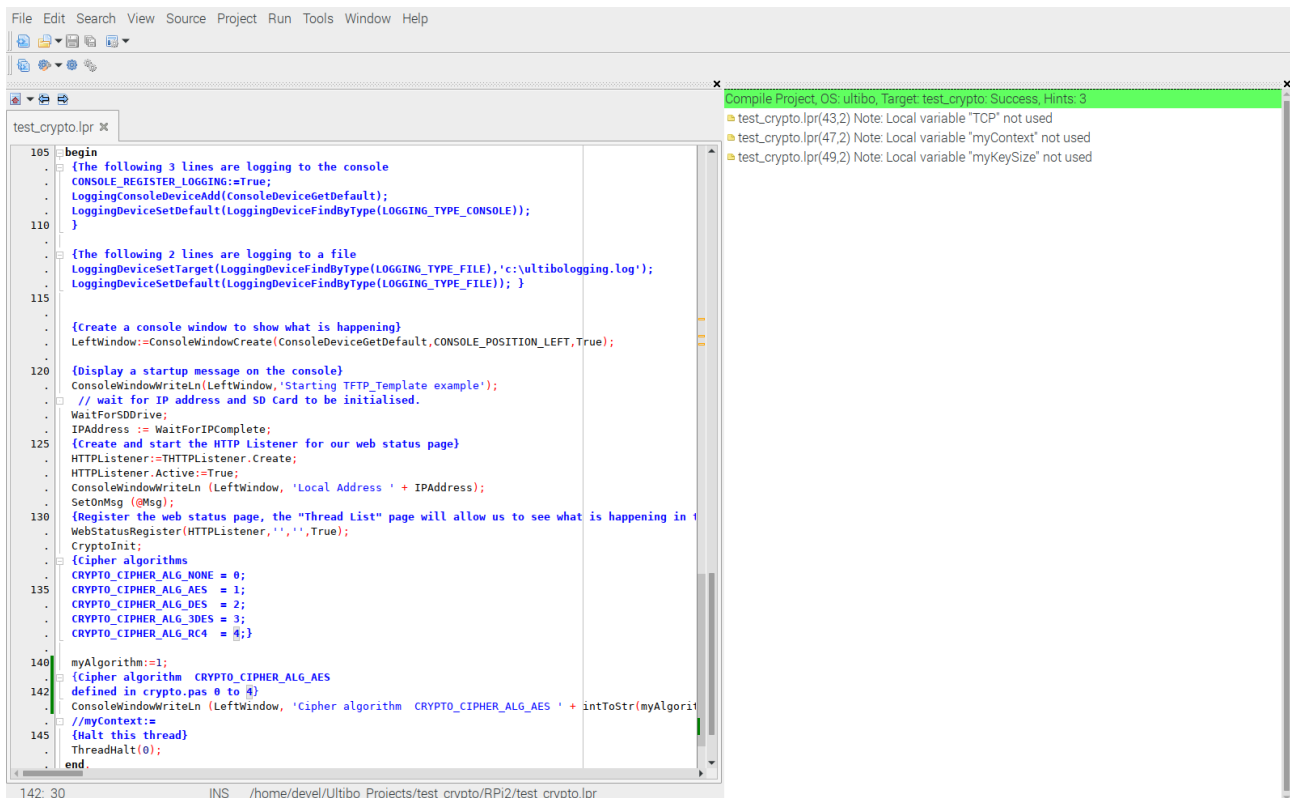
## crypto notes 05/02/20

### Starting with TFTP\_Template

\*\*\*\*\*Draft\*\*\*\*\*

Started with the file from “TFTP\_Template.lpr” to create “test\_crypto.lpr” & “test\_crypto.lpi”  
In addition this needs uTFTP.pas, upker7.sh, and cmdstftp.

Compile the project with “Run/Compile” or “Run/Clean up and Build”.



```
File Edit Search View Source Project Run Tools Window Help
test_crypto.lpr
105 begin
106 {The following 3 lines are logging to the console
107 .
108 .
109 .
110 .
111 .
112 .
113 .
114 .
115 .
116 .
117 .
118 .
119 .
120 .
121 .
122 .
123 .
124 .
125 .
126 .
127 .
128 .
129 .
130 .
131 .
132 .
133 .
134 .
135 .
136 .
137 .
138 .
139 .
140 .
141 .
142 .
143 .
144 .
145 .
146 .
147 .
148 .
149 .
150 .
151 .
152 .
153 .
154 .
155 .
156 .
157 .
158 .
159 .
160 .
161 .
162 .
163 .
164 .
165 .
166 .
167 .
168 .
169 .
170 .
171 .
172 .
173 .
174 .
175 .
176 .
177 .
178 .
179 .
180 .
181 .
182 .
183 .
184 .
185 .
186 .
187 .
188 .
189 .
190 .
191 .
192 .
193 .
194 .
195 .
196 .
197 .
198 .
199 .
200 .
201 .
202 .
203 .
204 .
205 .
206 .
207 .
208 .
209 .
210 .
211 .
212 .
213 .
214 .
215 .
216 .
217 .
218 .
219 .
220 .
221 .
222 .
223 .
224 .
225 .
226 .
227 .
228 .
229 .
230 .
231 .
232 .
233 .
234 .
235 .
236 .
237 .
238 .
239 .
240 .
241 .
242 .
243 .
244 .
245 .
246 .
247 .
248 .
249 .
250 .
251 .
252 .
253 .
254 .
255 .
256 .
257 .
258 .
259 .
260 .
261 .
262 .
263 .
264 .
265 .
266 .
267 .
268 .
269 .
270 .
271 .
272 .
273 .
274 .
275 .
276 .
277 .
278 .
279 .
280 .
281 .
282 .
283 .
284 .
285 .
286 .
287 .
288 .
289 .
290 .
291 .
292 .
293 .
294 .
295 .
296 .
297 .
298 .
299 .
300 .
301 .
302 .
303 .
304 .
305 .
306 .
307 .
308 .
309 .
310 .
311 .
312 .
313 .
314 .
315 .
316 .
317 .
318 .
319 .
320 .
321 .
322 .
323 .
324 .
325 .
326 .
327 .
328 .
329 .
330 .
331 .
332 .
333 .
334 .
335 .
336 .
337 .
338 .
339 .
340 .
341 .
342 .
343 .
344 .
345 .
346 .
347 .
348 .
349 .
350 .
351 .
352 .
353 .
354 .
355 .
356 .
357 .
358 .
359 .
360 .
361 .
362 .
363 .
364 .
365 .
366 .
367 .
368 .
369 .
370 .
371 .
372 .
373 .
374 .
375 .
376 .
377 .
378 .
379 .
380 .
381 .
382 .
383 .
384 .
385 .
386 .
387 .
388 .
389 .
390 .
391 .
392 .
393 .
394 .
395 .
396 .
397 .
398 .
399 .
400 .
401 .
402 .
403 .
404 .
405 .
406 .
407 .
408 .
409 .
410 .
411 .
412 .
413 .
414 .
415 .
416 .
417 .
418 .
419 .
420 .
421 .
422 .
423 .
424 .
425 .
426 .
427 .
428 .
429 .
430 .
431 .
432 .
433 .
434 .
435 .
436 .
437 .
438 .
439 .
440 .
441 .
442 .
443 .
444 .
445 .
446 .
447 .
448 .
449 .
450 .
451 .
452 .
453 .
454 .
455 .
456 .
457 .
458 .
459 .
460 .
461 .
462 .
463 .
464 .
465 .
466 .
467 .
468 .
469 .
470 .
471 .
472 .
473 .
474 .
475 .
476 .
477 .
478 .
479 .
480 .
481 .
482 .
483 .
484 .
485 .
486 .
487 .
488 .
489 .
490 .
491 .
492 .
493 .
494 .
495 .
496 .
497 .
498 .
499 .
500 .
501 .
502 .
503 .
504 .
505 .
506 .
507 .
508 .
509 .
510 .
511 .
512 .
513 .
514 .
515 .
516 .
517 .
518 .
519 .
520 .
521 .
522 .
523 .
524 .
525 .
526 .
527 .
528 .
529 .
530 .
531 .
532 .
533 .
534 .
535 .
536 .
537 .
538 .
539 .
540 .
541 .
542 .
543 .
544 .
545 .
546 .
547 .
548 .
549 .
550 .
551 .
552 .
553 .
554 .
555 .
556 .
557 .
558 .
559 .
560 .
561 .
562 .
563 .
564 .
565 .
566 .
567 .
568 .
569 .
570 .
571 .
572 .
573 .
574 .
575 .
576 .
577 .
578 .
579 .
580 .
581 .
582 .
583 .
584 .
585 .
586 .
587 .
588 .
589 .
590 .
591 .
592 .
593 .
594 .
595 .
596 .
597 .
598 .
599 .
600 .
601 .
602 .
603 .
604 .
605 .
606 .
607 .
608 .
609 .
610 .
611 .
612 .
613 .
614 .
615 .
616 .
617 .
618 .
619 .
620 .
621 .
622 .
623 .
624 .
625 .
626 .
627 .
628 .
629 .
630 .
631 .
632 .
633 .
634 .
635 .
636 .
637 .
638 .
639 .
640 .
641 .
642 .
643 .
644 .
645 .
646 .
647 .
648 .
649 .
650 .
651 .
652 .
653 .
654 .
655 .
656 .
657 .
658 .
659 .
660 .
661 .
662 .
663 .
664 .
665 .
666 .
667 .
668 .
669 .
670 .
671 .
672 .
673 .
674 .
675 .
676 .
677 .
678 .
679 .
680 .
681 .
682 .
683 .
684 .
685 .
686 .
687 .
688 .
689 .
690 .
691 .
692 .
693 .
694 .
695 .
696 .
697 .
698 .
699 .
700 .
701 .
702 .
703 .
704 .
705 .
706 .
707 .
708 .
709 .
710 .
711 .
712 .
713 .
714 .
715 .
716 .
717 .
718 .
719 .
720 .
721 .
722 .
723 .
724 .
725 .
726 .
727 .
728 .
729 .
730 .
731 .
732 .
733 .
734 .
735 .
736 .
737 .
738 .
739 .
740 .
741 .
742 .
743 .
744 .
745 .
746 .
747 .
748 .
749 .
750 .
751 .
752 .
753 .
754 .
755 .
756 .
757 .
758 .
759 .
760 .
761 .
762 .
763 .
764 .
765 .
766 .
767 .
768 .
769 .
770 .
771 .
772 .
773 .
774 .
775 .
776 .
777 .
778 .
779 .
780 .
781 .
782 .
783 .
784 .
785 .
786 .
787 .
788 .
789 .
790 .
791 .
792 .
793 .
794 .
795 .
796 .
797 .
798 .
799 .
800 .
801 .
802 .
803 .
804 .
805 .
806 .
807 .
808 .
809 .
810 .
811 .
812 .
813 .
814 .
815 .
816 .
817 .
818 .
819 .
820 .
821 .
822 .
823 .
824 .
825 .
826 .
827 .
828 .
829 .
830 .
831 .
832 .
833 .
834 .
835 .
836 .
837 .
838 .
839 .
840 .
841 .
842 .
843 .
844 .
845 .
846 .
847 .
848 .
849 .
850 .
851 .
852 .
853 .
854 .
855 .
856 .
857 .
858 .
859 .
860 .
861 .
862 .
863 .
864 .
865 .
866 .
867 .
868 .
869 .
870 .
871 .
872 .
873 .
874 .
875 .
876 .
877 .
878 .
879 .
880 .
881 .
882 .
883 .
884 .
885 .
886 .
887 .
888 .
889 .
890 .
891 .
892 .
893 .
894 .
895 .
896 .
897 .
898 .
899 .
900 .
901 .
902 .
903 .
904 .
905 .
906 .
907 .
908 .
909 .
910 .
911 .
912 .
913 .
914 .
915 .
916 .
917 .
918 .
919 .
920 .
921 .
922 .
923 .
924 .
925 .
926 .
927 .
928 .
929 .
930 .
931 .
932 .
933 .
934 .
935 .
936 .
937 .
938 .
939 .
940 .
941 .
942 .
943 .
944 .
945 .
946 .
947 .
948 .
949 .
950 .
951 .
952 .
953 .
954 .
955 .
956 .
957 .
958 .
959 .
960 .
961 .
962 .
963 .
964 .
965 .
966 .
967 .
968 .
969 .
970 .
971 .
972 .
973 .
974 .
975 .
976 .
977 .
978 .
979 .
980 .
981 .
982 .
983 .
984 .
985 .
986 .
987 .
988 .
989 .
990 .
991 .
992 .
993 .
994 .
995 .
996 .
997 .
998 .
999 .
1000 .
end.
```

Compile Project OS: ultibo, Target: test\_crypto, Success, Hints: 3

- test\_crypto.lpr(43,2) Note: Local variable "TCP" not used
- test\_crypto.lpr(47,2) Note: Local variable "myContext" not used
- test\_crypto.lpr(49,2) Note: Local variable "myKeySize" not used

142: 30 INS /home/devel/Ultibo\_Projects/test\_crypto/RPi2/test\_crypto.lpr

Once the Green bar is displayed it can be transfer to the Ultibo System.

After adding APICrypto.pas

In test\_crypto.lpt in

**var**

**AESECBKey:PByte;**

**AESECBData:PByte;**

**AESECBAESKey:TAESKey;**

**AESCBCKey:PByte;**

**AESCBData:PByte;**

**AESCBCVector:PByte;**

**//Context:PBigIntContext;**

**Cipher:PCipherContext;**

**key:String;**

**Data:String;**

**Actual:String;**

**PData:PString;**

**Datalen:LongWord;**

With the addition of code

**ConsoleWindowWriteLn (LeftWindow, '');**

**ConsoleWindowWriteLn (LeftWindow, 'AESEncryptBlock (128bit)');**

**ConsoleWindowWriteLn (LeftWindow, 'Electronic Codebook (ECB)');**

**AESECBKey:=AllocMem(AES\_KEY\_SIZE128);**

**StringToBytes('2b7e151628aed2a6abf7158809cf4f3c',PByte(AESECBKey),AES\_**  
**KEY\_SIZE128);**

**AESECBData:=AllocMem(AES\_BLOCK\_SIZE);**

**StringToBytes('6bc1bee22e409f96e93d7e117393172a',PByte(AESECBData),AES**  
**\_BLOCK\_SIZE);**

**AESKeySetup(AESECBKey,AES\_KEY\_SIZE128,@AESECBAESKey);**

**AESEncryptBlock(AESECBData,AESECBData,@AESECBAESKey);**

**Actual:=BytesToString(PByte(AESECBData),AES\_BLOCK\_SIZE);**

**ConsoleWindowWriteLn (LeftWindow, 'Key: '**  
**+ '2b7e151628aed2a6abf7158809cf4f3c');**

**ConsoleWindowWriteLn (LeftWindow, 'Data: '**  
**+ '6bc1bee22e409f96e93d7e117393172a');**

**ConsoleWindowWriteLn (LeftWindow, 'Actual: ' + Actual);**

**FreeMem(AESECBKey);**

**FreeMem(AESECBData);**

**ConsoleWindowWriteLn (LeftWindow, '');**

**ConsoleWindowWriteLn (LeftWindow, 'AESEncryptBlock (192bit)');**

**ConsoleWindowWriteLn (LeftWindow, 'Electronic Codebook (ECB)');**

**AESECBKey:=AllocMem(AES\_KEY\_SIZE192);**

**StringToBytes('8e73b0f7da0e6452c810f32b809079e562f8ead2522c6b7b',PByte(AESECBKey),AES\_KEY\_SIZE192);**

**AESECBData:=AllocMem(AES\_BLOCK\_SIZE);**

**StringToBytes('6bc1bee22e409f96e93d7e117393172a',PByte(AESECBData),AES\_BLOCK\_SIZE);**

**AESKeySetup(AESECBKey,AES\_KEY\_SIZE192,@AESECBAESKey);**

**AESEncryptBlock(AESECBData,AESECBData,@AESECBAESKey);**

**Actual:=BytesToString(PByte(AESECBData),AES\_BLOCK\_SIZE);**

**ConsoleWindowWriteLn (LeftWindow, 'Key: ' + '8e73b0f7da0e6452c810f32b809079e562f8ead2522c6b7b');**

**ConsoleWindowWriteLn (LeftWindow, 'Data: ' + '6bc1bee22e409f96e93d7e117393172a');**

**ConsoleWindowWriteLn (LeftWindow, 'Actual: ' + Actual);**

**FreeMem(AESECBKey);**

**FreeMem(AESECBData);**

**ConsoleWindowWriteLn (LeftWindow, '');**

**ConsoleWindowWriteLn (LeftWindow, 'AESEncryptBlock (256bit)');**

**ConsoleWindowWriteLn (LeftWindow, 'Electronic Codebook (ECB)');**

**AESECBKey:=AllocMem(AES\_KEY\_SIZE256);**

**StringToBytes('603deb1015ca71be2b73aef0857d77811f352c073b6108d72d9810a30914dff4',PByte(AESECBKey),AES\_KEY\_SIZE256);**

**AESECBData:=AllocMem(AES\_BLOCK\_SIZE);**

**StringToBytes('6bc1bee22e409f96e93d7e117393172a',PByte(AESECBData),AES\_BLOCK\_SIZE);**

**AESKeySetup(AESECBKey,AES\_KEY\_SIZE256,@AESECBAESKey);**

**AESEncryptBlock(AESECBData,AESECBData,@AESECBAESKey);**

**Actual:=BytesToString(PByte(AESECBData),AES\_BLOCK\_SIZE);**

**ConsoleWindowWriteLn (LeftWindow, 'Key: ' + '603deb1015ca71be2b73aef0857d77811f352c073b6108d72d9810a30914dff4');**

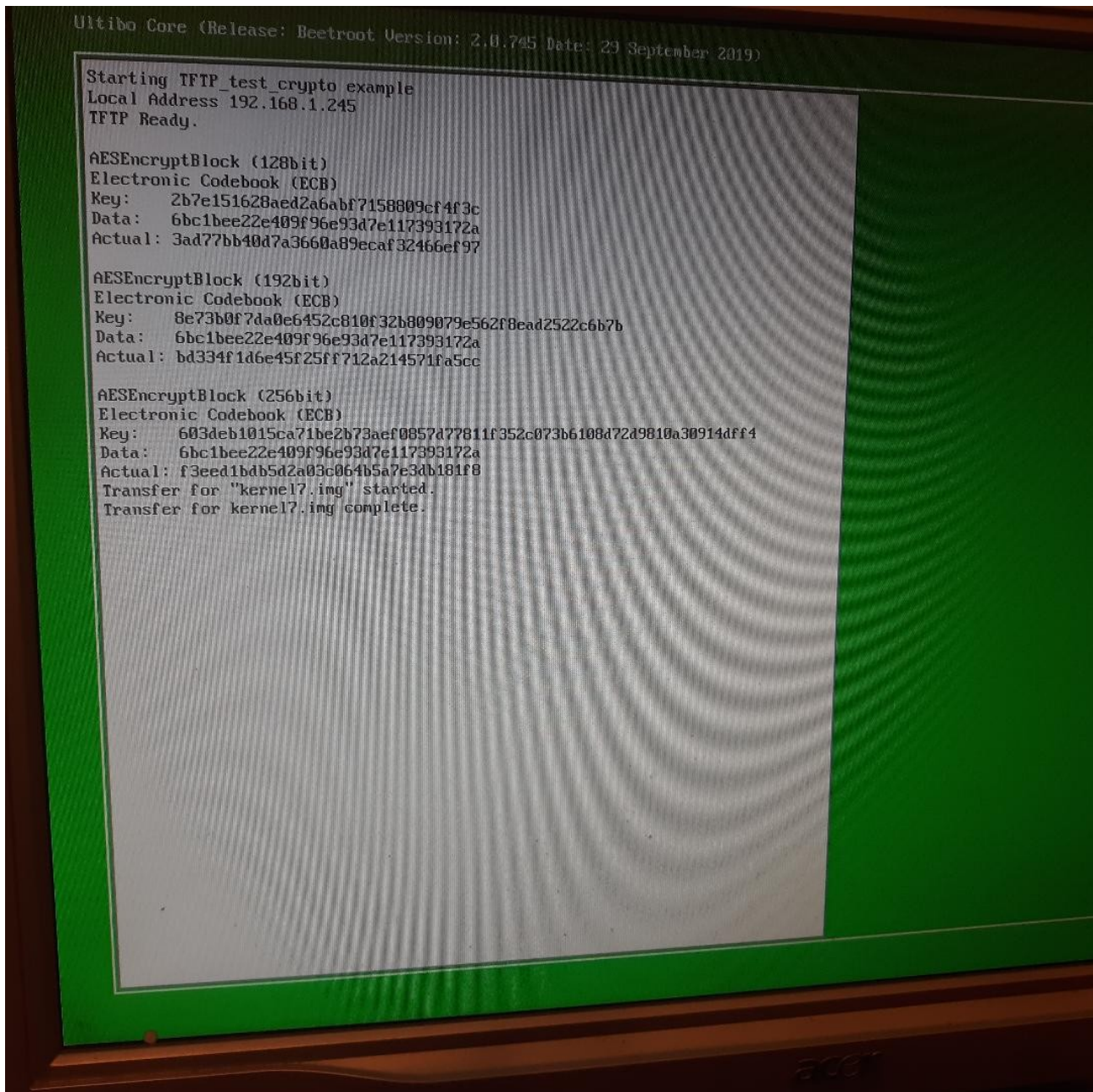
**ConsoleWindowWriteLn (LeftWindow, 'Data: ' + '6bc1bee22e409f96e93d7e117393172a');**

**ConsoleWindowWriteLn (LeftWindow, 'Actual: ' + Actual);**

**FreeMem(AESECBKey);**

**FreeMem(AESECBData);**

./upker.sh



Now the results match the results on <http://192.168.1.245/status/cryptoapi/>

(219 unread) - develone x ultibo.org - New posts x Ultibo Core (Release: Bee x +

File | /home/devel/ultibo-web/Ultibo%20Core%20(Release%3A%20Beetroot%20Version%3A%202.0.745%20Date%3A... Q ☆

AES Cipher Tests

Test: AESEncryptBlock (128bit)

Key: 0x2b7e151628aed2a6abf7158809cf4f3c

Data: 0x6bc1bee22e409f96e93d7e117393172a

Vector: (None)

Mode: Electronic Codebook (ECB)

Expected: 3ad77bb40d7a3660a89ecaf32466ef97

Actual: 3ad77bb40d7a3660a89ecaf32466ef97

Result: Correct

Test: AESEncryptBlock (192bit)

Key: 0x8e73b0f7da0e6452c810f32b809079e562f8ead2522c6b7b

Data: 0x6bc1bee22e409f96e93d7e117393172a

Vector: (None)

Mode: Electronic Codebook (ECB)

Expected: bd334f1d6e45f25ff712a214571fa5cc

Actual: bd334f1d6e45f25ff712a214571fa5cc

Result: Correct

Test: AESEncryptBlock (256bit)

Key: 0x603deb1015ca71be2b73aef0857d77811f352c073b6108d72d9810a30914dffa

Data: 0x6bc1bee22e409f96e93d7e117393172a

Vector: (None)

Mode: Electronic Codebook (ECB)

Expected: f3eed1bdb5d2a03c064b5a7e3db181f8

Actual: f3eed1bdb5d2a03c064b5a7e3db181f8

Result: Correct

AESECB.jpeg ^

Show all x

Ultibo Core (Release: Beetroot Version: 2.0.745 Date: 29 September 2019)

```
Starting TFTP Template example
Local Address 192.168.1.245
TFTP Ready.
Cipher algorithm CRYPTO_CIPHER_ALG_AES_1
Transfer for "kernel7.img" started.
Transfer for kernel7.img complete.
```

acer

shell1



```
File Edit Tabs Help
devel@mypi3-15:~/Ultibo_Projects/test_crypto/RPi2 $ telnet 192.168.1.245
```

shell2

```
File Edit Tabs Help
29-3-20 02:24:18      3798568 start_x.elf
29-3-20 02:24:18      3145850 t
29-3-20 02:24:20       635016 teapot.obj.dat
29-3-20 02:23:56         24 testfile
29-3-20 02:24:20     27983872 test.h264
29-3-20 02:24:24        500 test.html
10-4-20 16:23:58       7848 test.j2k
6-4-20 17:37:26     196730 test_wr.bmp
29-3-20 02:24:24       1718 ultibologging.log
29-3-20 02:24:24     27983872 v1.h264
29-3-20 02:24:30     1002763 v2.h264
29-3-20 02:24:30    <DIR>      www
2-4-20 17:31:26       65596 red.pgm
2-4-20 17:31:38       65596 grn.pgm
2-4-20 17:31:52       65596 blu.pgm
6-4-20 11:23:30        1024 Sred.bin
6-4-20 11:23:34        1024 Sgrn.bin
6-4-20 11:23:36     262144 rcgrn.bin
6-4-20 11:23:38        1024 Sblu.bin
6-4-20 11:23:38     262144 rcblu.bin
      69 file(s) 136527430 bytes
      2 dir(s)

C:\>
```

Webstatus



Ultibo Core (Release: Beetroot Version: 2.0.745 Date: 29 September 2019)

General	General	
Platform		
Memory	Release Name:	Beetroot
Heap Blocks	Release Version:	2.0.745
CPU	Release Date:	29 September 2019
FPU		
GPU	Time (Local):	30-12-99 00:00:08
RTL	Time (UTC):	30-12-99 00:00:08
Clock		
Locale	Timezone:	UTC
Threading		
Thread List	Daylight Start:	None
Scheduler	Daylight Date:	N/A
Devices		
Drivers	Standard Start:	None
Handles	Standard Date:	N/A
USB		
MMC / SD	Uptime:	0 days 00:00:08
Network		
Storage		
Filesystem		
Disk Cache		
Keyboard		
Mouse		
Framebuffer		