HACK.LU 2025

BREAK. BUILD. SHARE.

Inbar Raz

Reversing a Payphone for Fun but no Profit

Introduction:

#WTF?

#whoami

- I'm a geek.
- I'm a reverser.
- I'm a hacker.
- I'm a retro-computing collector and restorer.
- I'm (too) curious.

And…

- I engage technicians.

@inbarraz / @zenitysec

-HIRING AI RESEARCHERS-

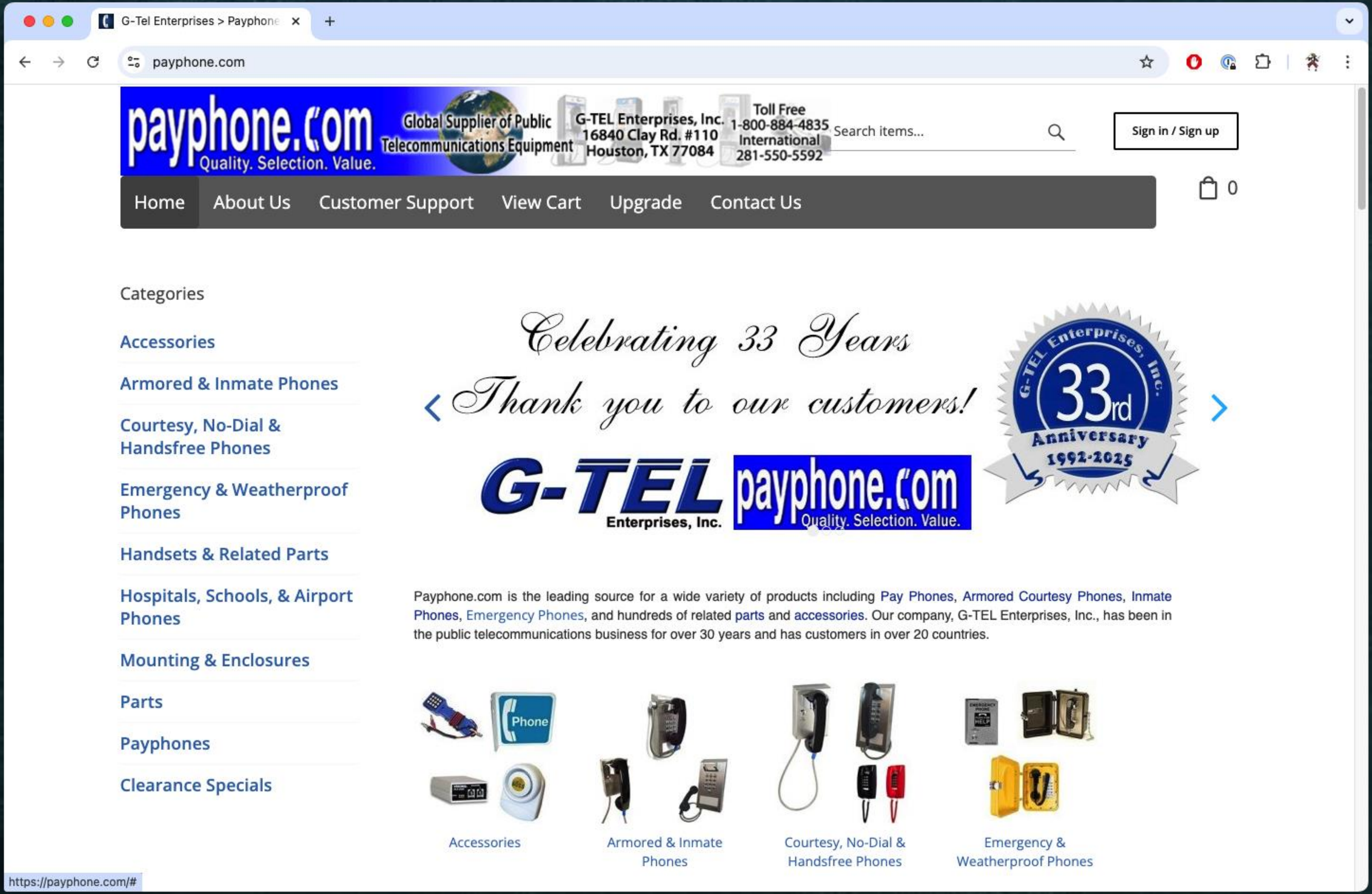
TA0043:

Reconnaissance

Preliminary Research

- Looked for various payphone manuals.
- Guess what?

Preliminary Research



G-Tel Enterprises > Payphone

payphone.com

payphone.com Quality. Selection. Value.

Global Supplier of Public Telecommunications Equipment

G-TEL Enterprises, Inc.
16840 Clay Rd. #110
Houston, TX 77084

Toll Free
1-800-884-4835
International
281-550-5592

Search items...

Sign in / Sign up

0

Home | About Us | Customer Support | View Cart | Upgrade | Contact Us

Categories

- Accessories
- Armored & Inmate Phones
- Courtesy, No-Dial & Handsfree Phones
- Emergency & Weatherproof Phones
- Handsets & Related Parts
- Hospitals, Schools, & Airport Phones
- Mounting & Enclosures
- Parts
- Payphones
- Clearance Specials

Celebrating 33 Years

Thank you to our customers!

G-TEL Enterprises, Inc. payphone.com Quality. Selection. Value.

G-TEL Enterprises, Inc. 33rd Anniversary 1992-2025

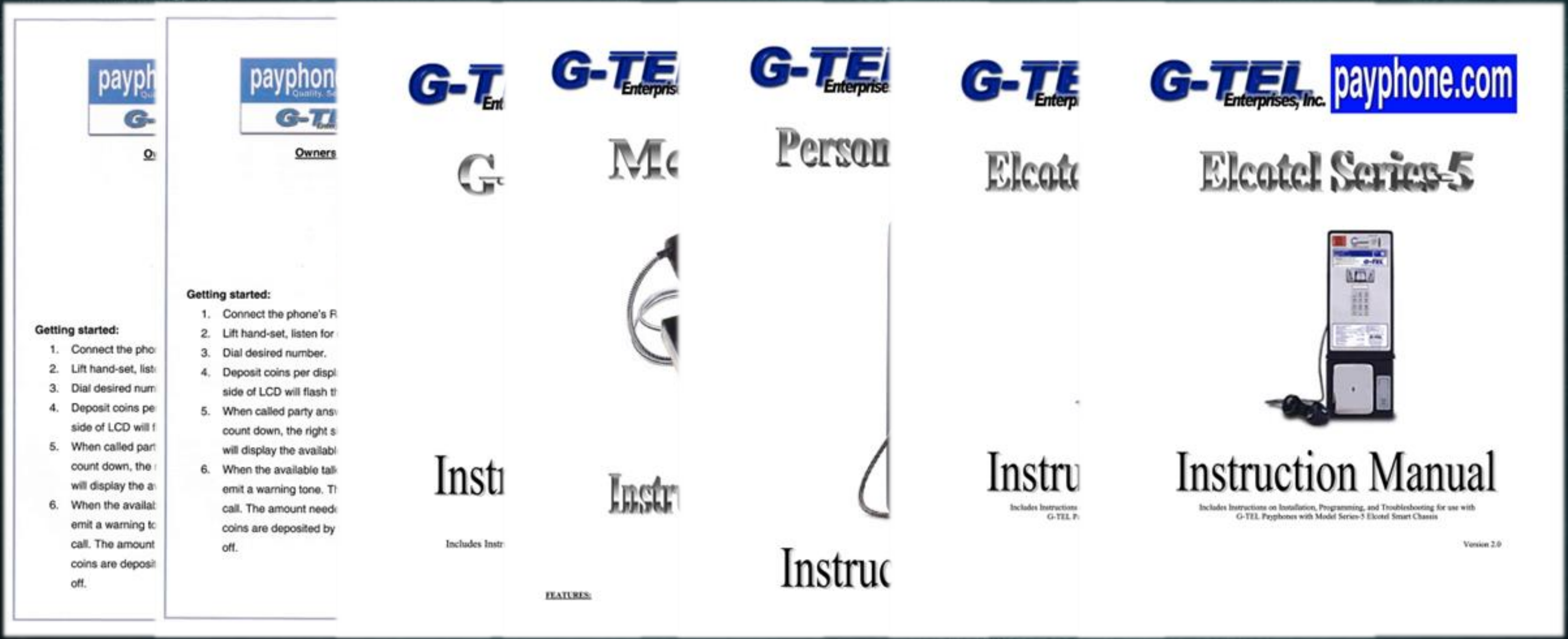
Payphone.com is the leading source for a wide variety of products including Pay Phones, Armored Courtesy Phones, Inmate Phones, Emergency Phones, and hundreds of related parts and accessories. Our company, G-TEL Enterprises, Inc., has been in the public telecommunications business for over 30 years and has customers in over 20 countries.

Accessories | Armored & Inmate Phones | Courtesy, No-Dial & Handsfree Phones | Emergency & Weatherproof Phones

https://payphone.com/#

Preliminary Research

- Has manuals for multiple models:



payph
Qu
G-
O

Getting started:

1. Connect the pho
2. Lift hand-set, list
3. Dial desired num
4. Deposit coins pe
side of LCD will f
5. When called part
count down, the
will display the a
6. When the availa
emit a warning to
call. The amount
coins are deposi
off.

payphon
Quality, S
G-TI
Owners

Getting started:

1. Connect the phone's R
2. Lift hand-set, listen for
3. Dial desired number.
4. Deposit coins per displ
side of LCD will flash th
5. When called party answ
count down, the right s
will display the availabl
6. When the available talk
emit a warning tone. Th
call. The amount need
coins are deposited by
off.

G-T
Ent
G
Instr
Includes Instr

G-TE
Enterpris
Mo
Instr
FEATURES:

G-TEI
Enterprise
Person
Instruc

G-TE
Enterp
Elcote
Instru
Includes Instructions
G-TEL P

G-TEL Enterprises, Inc. payphone.com

Elcotel Series-5

Instruction Manual

Includes Instructions on Installation, Programming, and Troubleshooting for use with G-TEL Payphones with Model Series-5 Elcotel Smart Chassis

Version 2.0

Preliminary Research

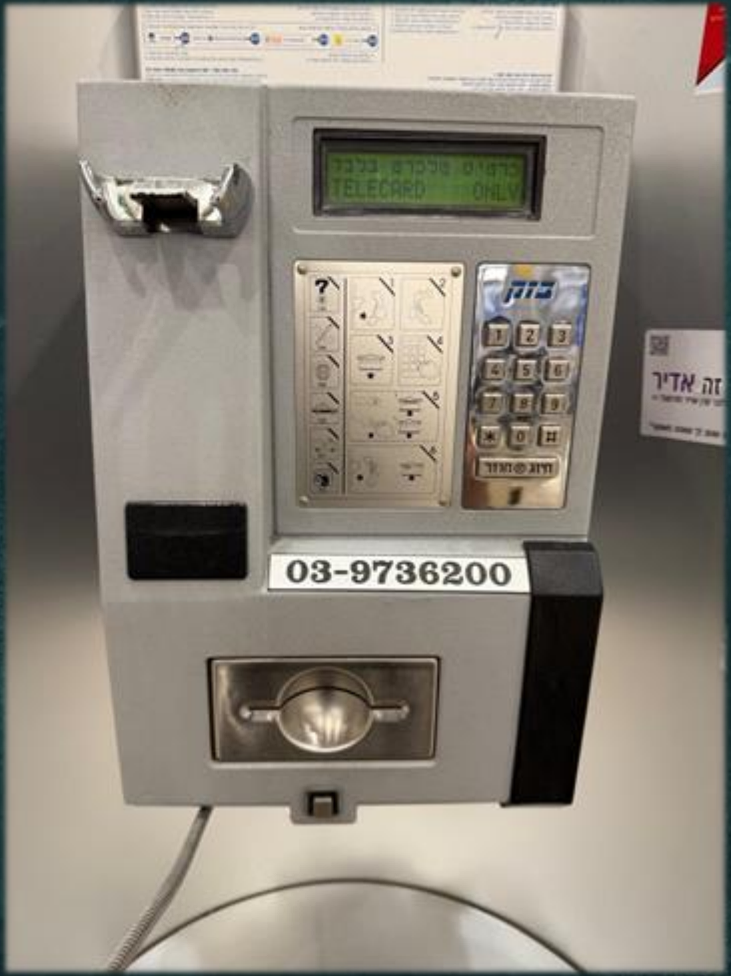
- Kept my eyes (and my camera) open.

Preliminary Research

- Kept my eyes (and my camera) open.

Preliminary Research

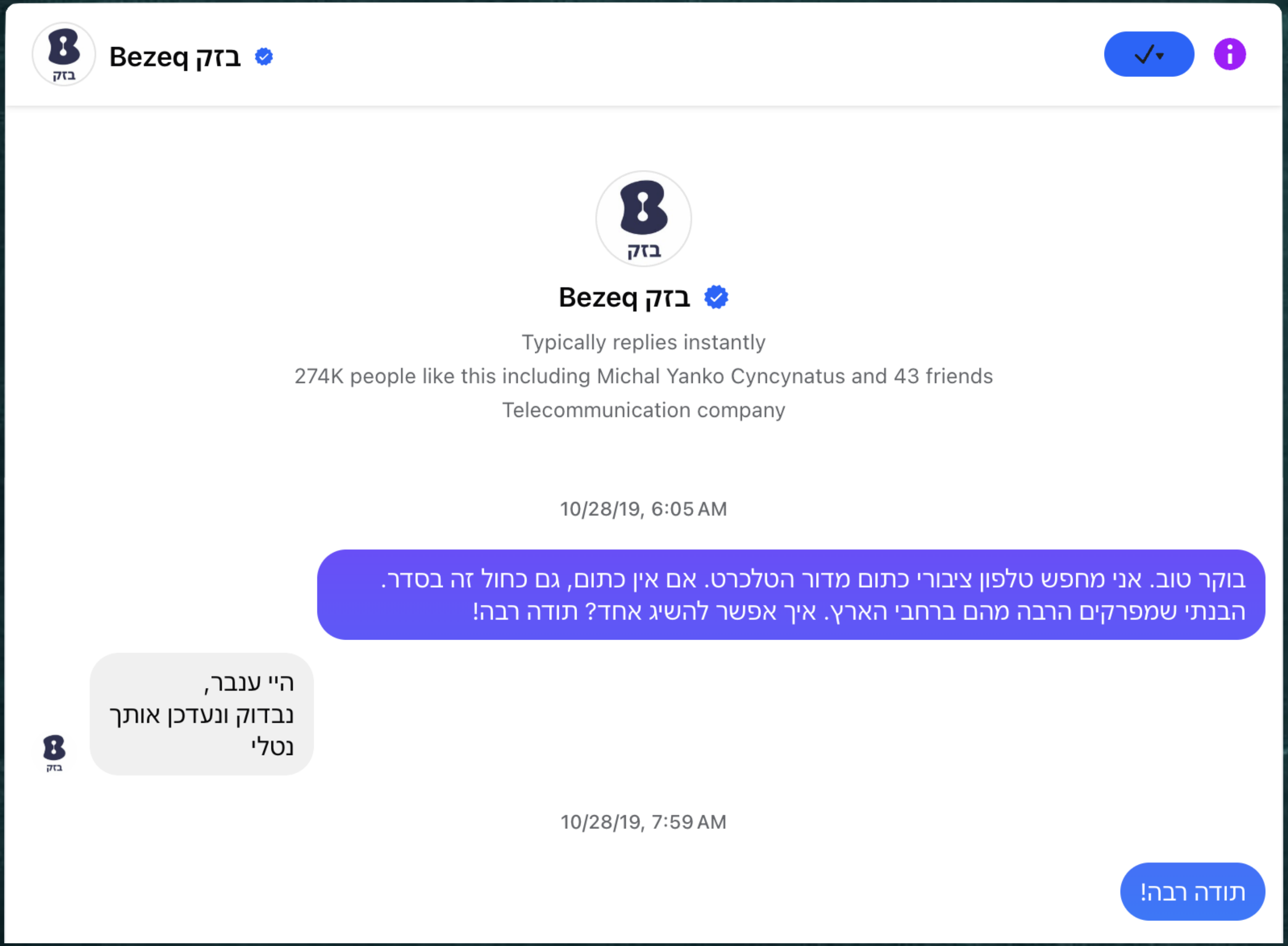
- Kept my eyes (and my camera) open.



19/05/2025
TLV

Acquisition

Plan A: Go to the source



Bezeq בזק

Bezeq בזק

Typically replies instantly

274K people like this including Michal Yanko Cyncynatus and 43 friends

Telecommunication company

10/28/19, 6:05 AM

בוקר טוב. אני מחפש טלפון ציבורי כתום מדור הטלכרט. אם אין כתום, גם כחול זה בסדר.
הבנתי שמפרקים הרבה מהם ברחבי הארץ. איך אפשר להשיג אחד? תודה רבה!

היי ענבר,
נבדוק ונעדכן אותך
נטלי

10/28/19, 7:59 AM

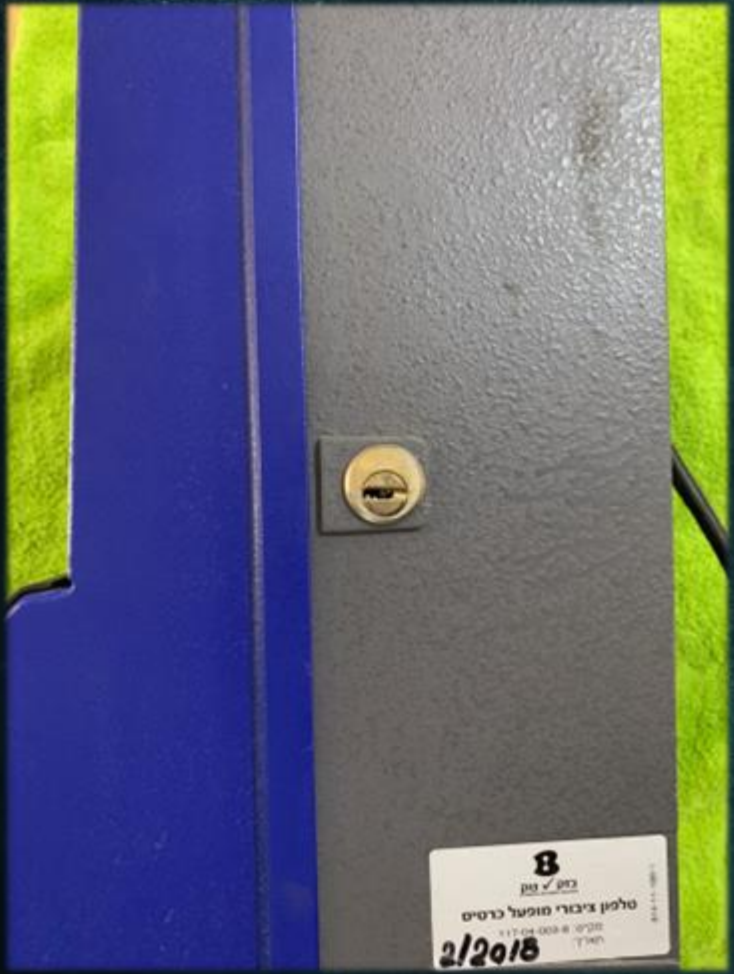
תודה רבה!

Plan B: Secondary Market

TA0001:

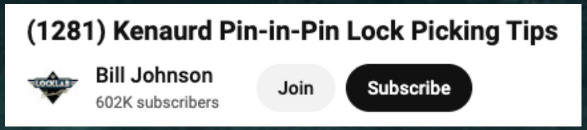
Initial Access

Chassis is locked



Yale Pin-in-Pin

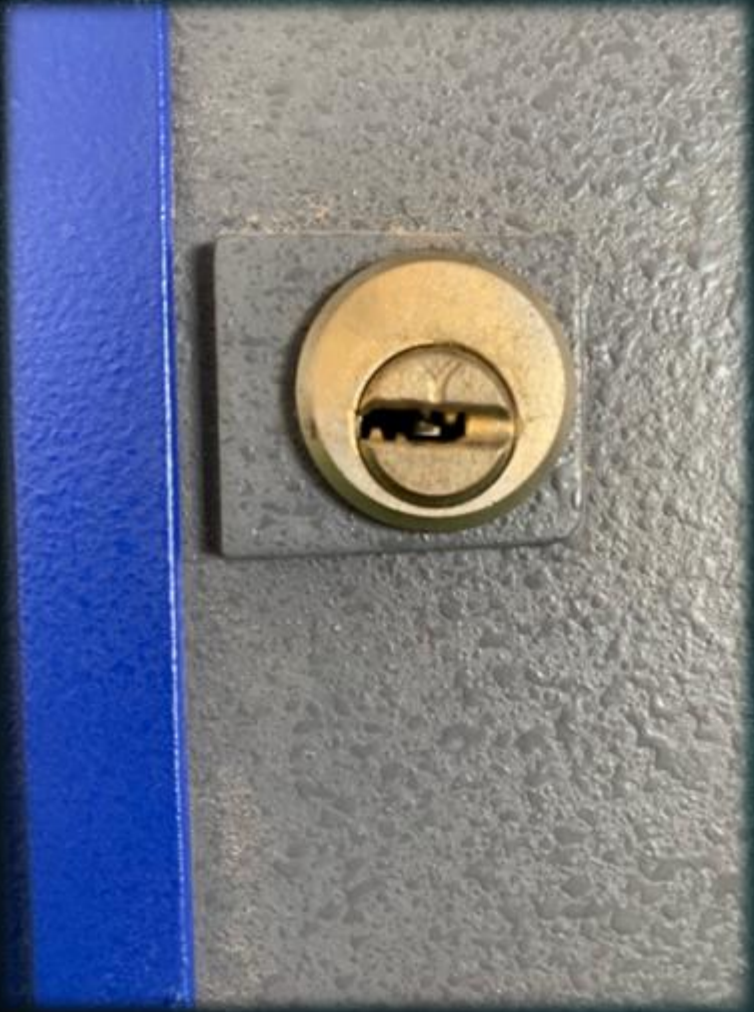
Chassis is locked



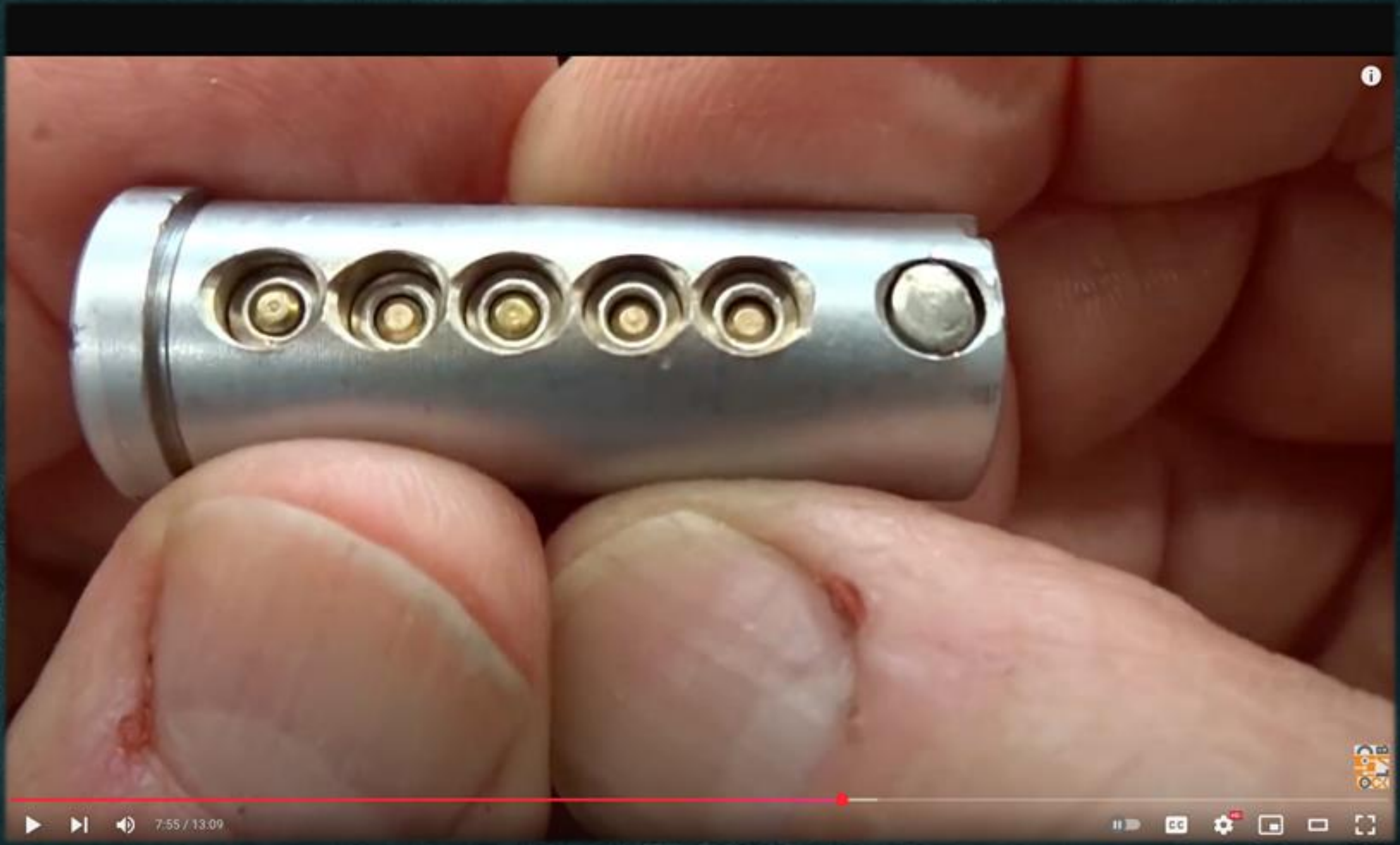
(1281) Kenaurd Pin-in-Pin Lock Picking Tips

Bill Johnson

602K subscribers



On the outside



On the inside

To the Rescue...

IT'S **ON!**

GET YOUR TICKET FOR **#DEFCAMP2019**

7th-8th Nov/2019

BUCHAREST, ROMANIA

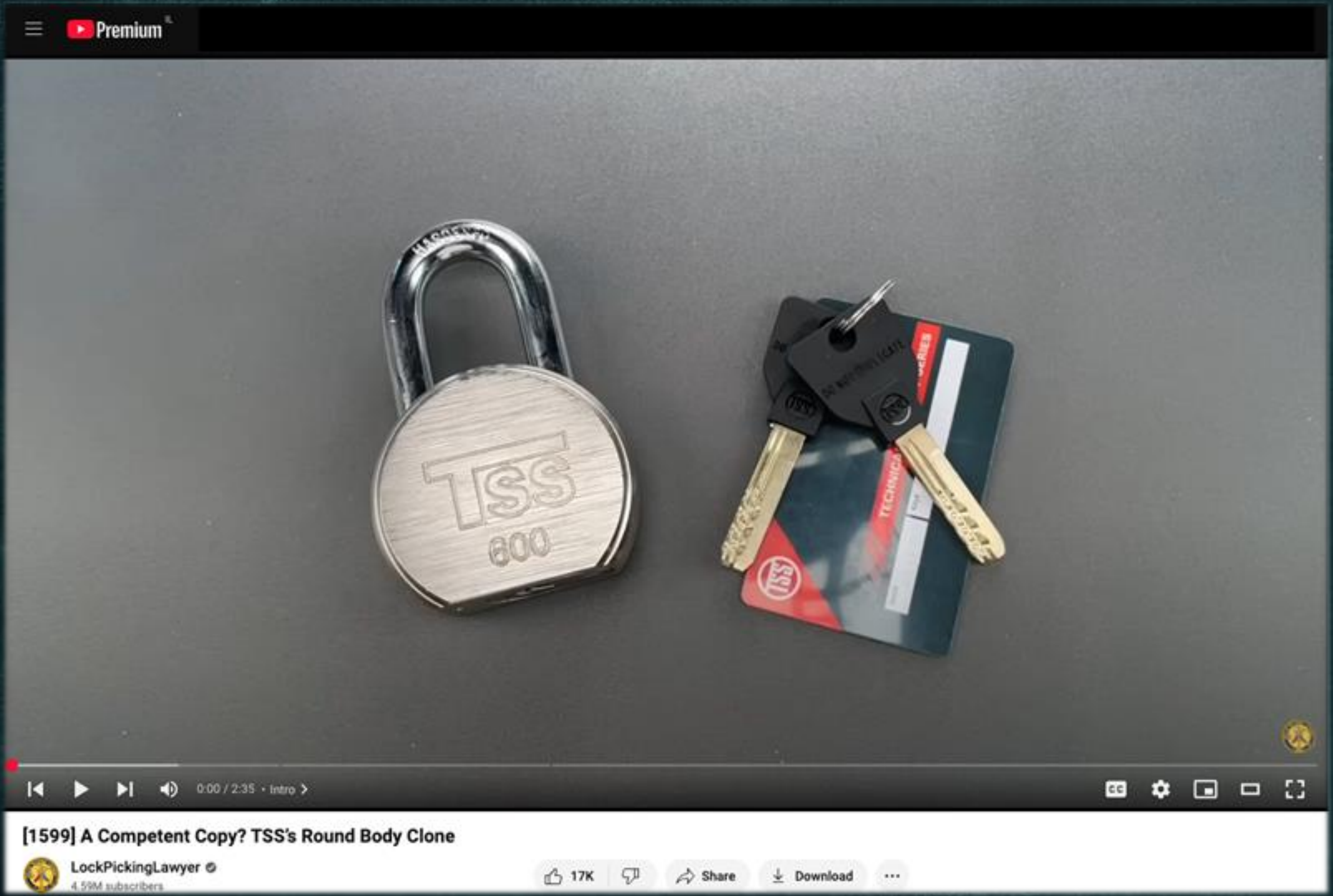
To the Rescue...

Lock Picking Village

DefCamp

Gabriel Cirlig

Learning a new Skill



[1599] A Competent Copy? TSS's Round Body Clone

Learning a new Skill

MUL-T-LOCK

And... you get the idea.

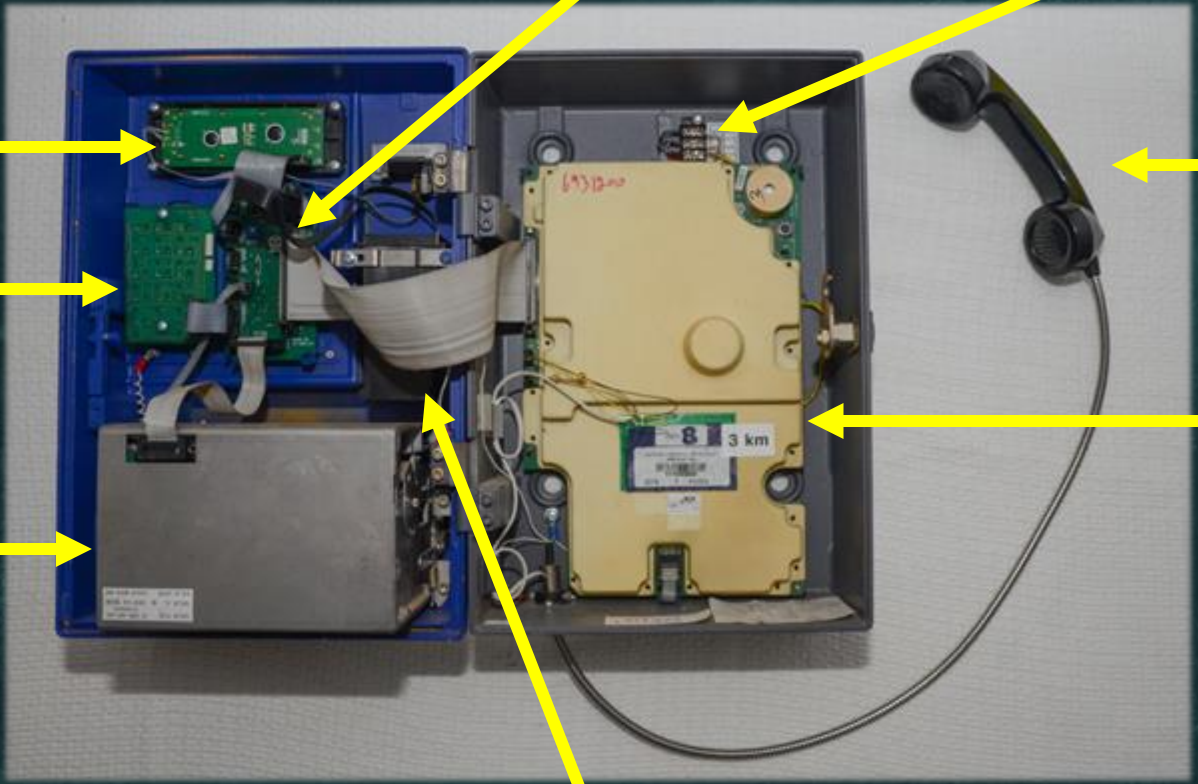
A FEW
MOMENTS LATER

Lo and Behold!

TA0007:

Discovery

An overview



Distribution Board

Phone Line

LCD

Earpiece

Keyboard

Motherboard

Card Reader

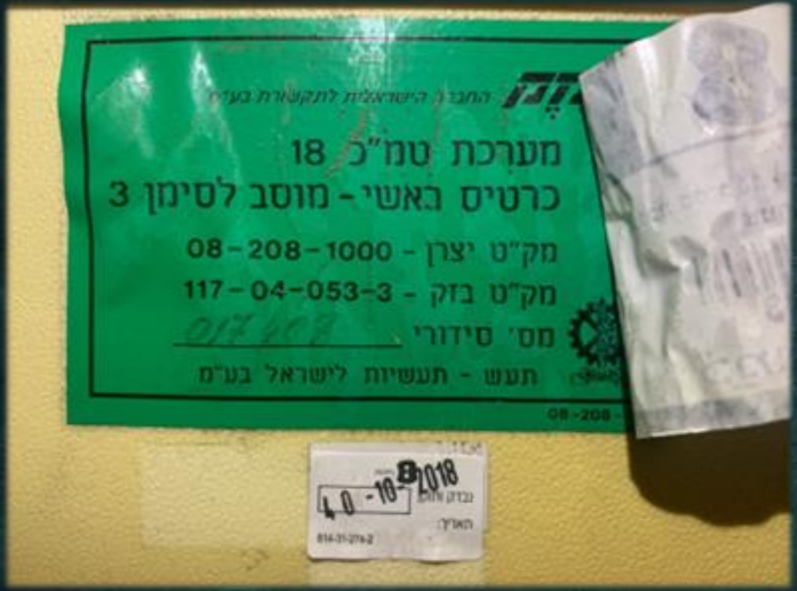
Backup Battery

Unexpected surprise

- If I had to guess who the manufacture was, I’d have a few immediate suspects.

Unexpected surprise

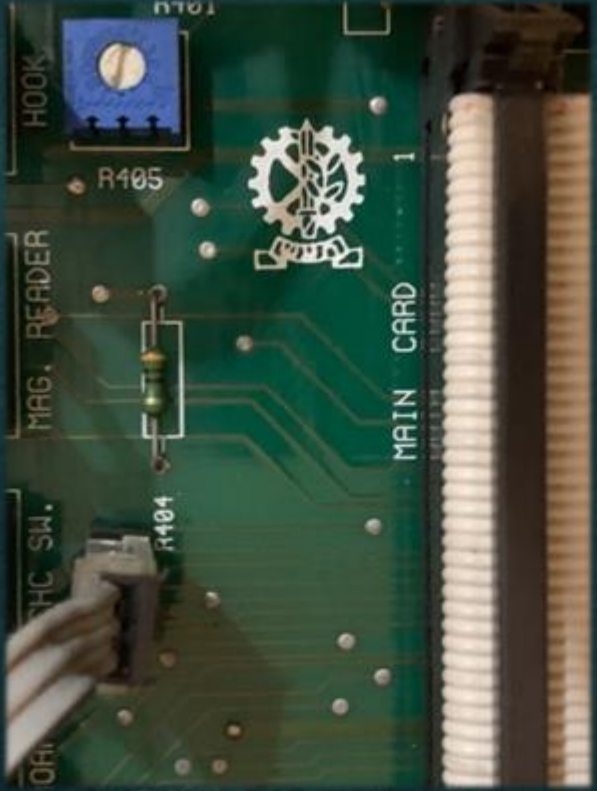
- If I had to guess who the manufacture was, I’d have a few immediate suspects.
- IMI was ***NOT*** one of them.


בזק החברה הישראלית לתקשורת בע"מ

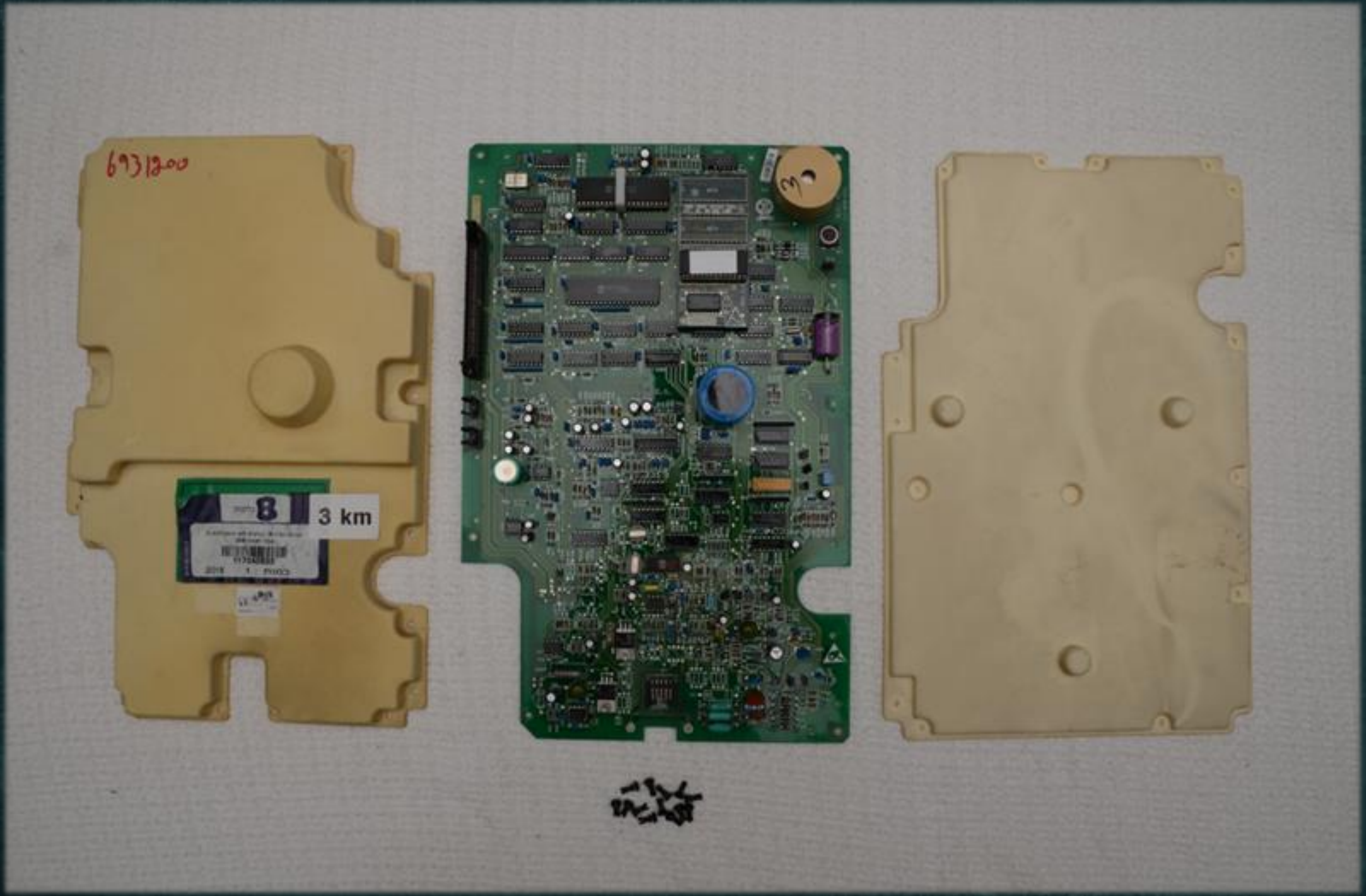
מערכת טמ"כ 18
כרטיס באשי - מוסב לסימן 3
מק"ט יצרן - 08-208-1000
מק"ט בזק - 117-04-053-3
מס' סידורי 017 407
תעש - תעשיות לישראל בע"מ

08-208-

10-10-2018
נבדק חשמלית
תאריך:
814-31-274-2

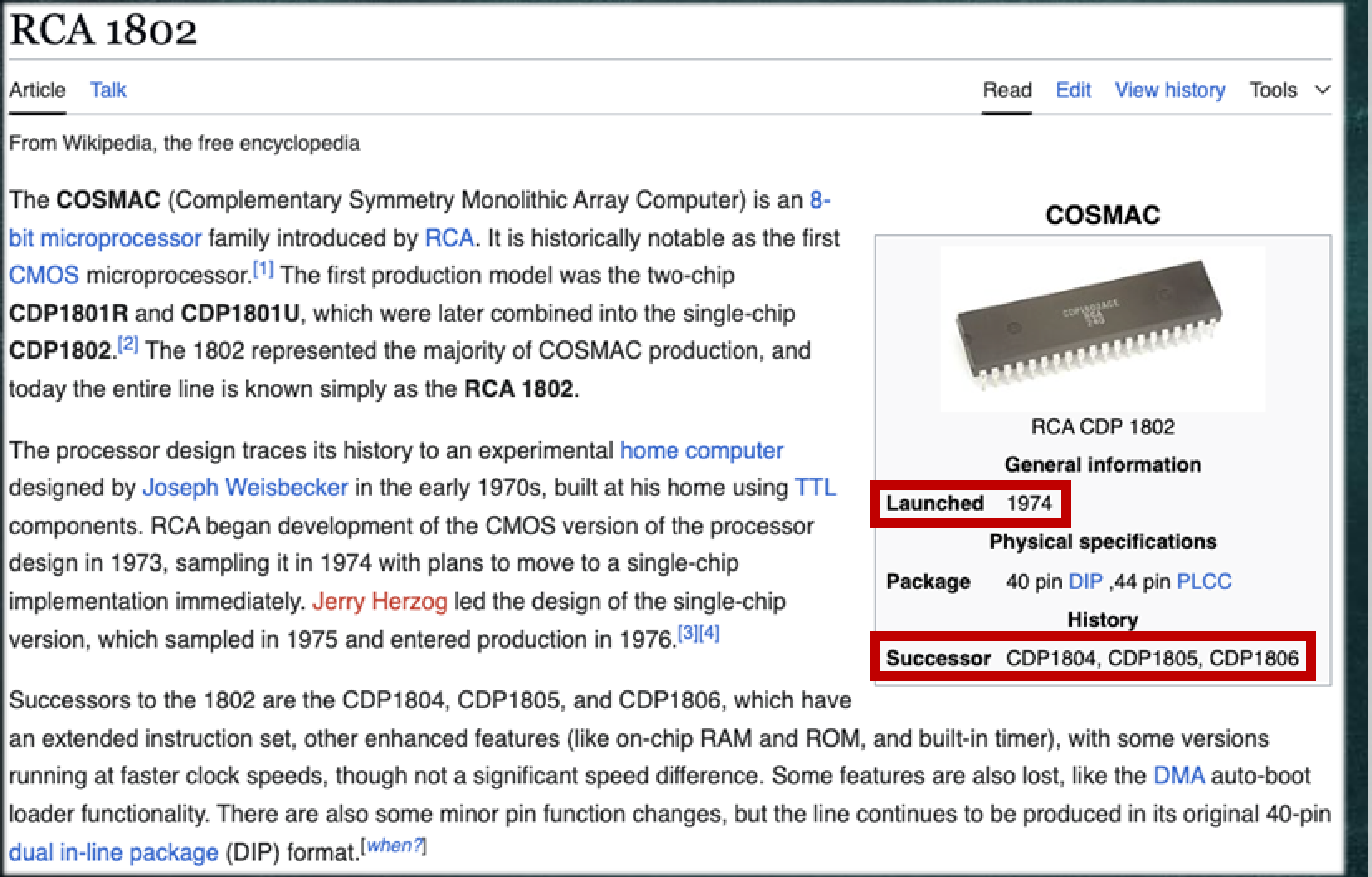


The Motherboard



The Motherboard

CPU Identification



RCA 1802

From Wikipedia, the free encyclopedia

The **COSMAC** (Complementary Symmetry Monolithic Array Computer) is an 8-bit microprocessor family introduced by RCA. It is historically notable as the first CMOS microprocessor.[1] The first production model was the two-chip **CDP1801R** and **CDP1801U**, which were later combined into the single-chip **CDP1802**.[2] The 1802 represented the majority of COSMAC production, and today the entire line is known simply as the **RCA 1802**.

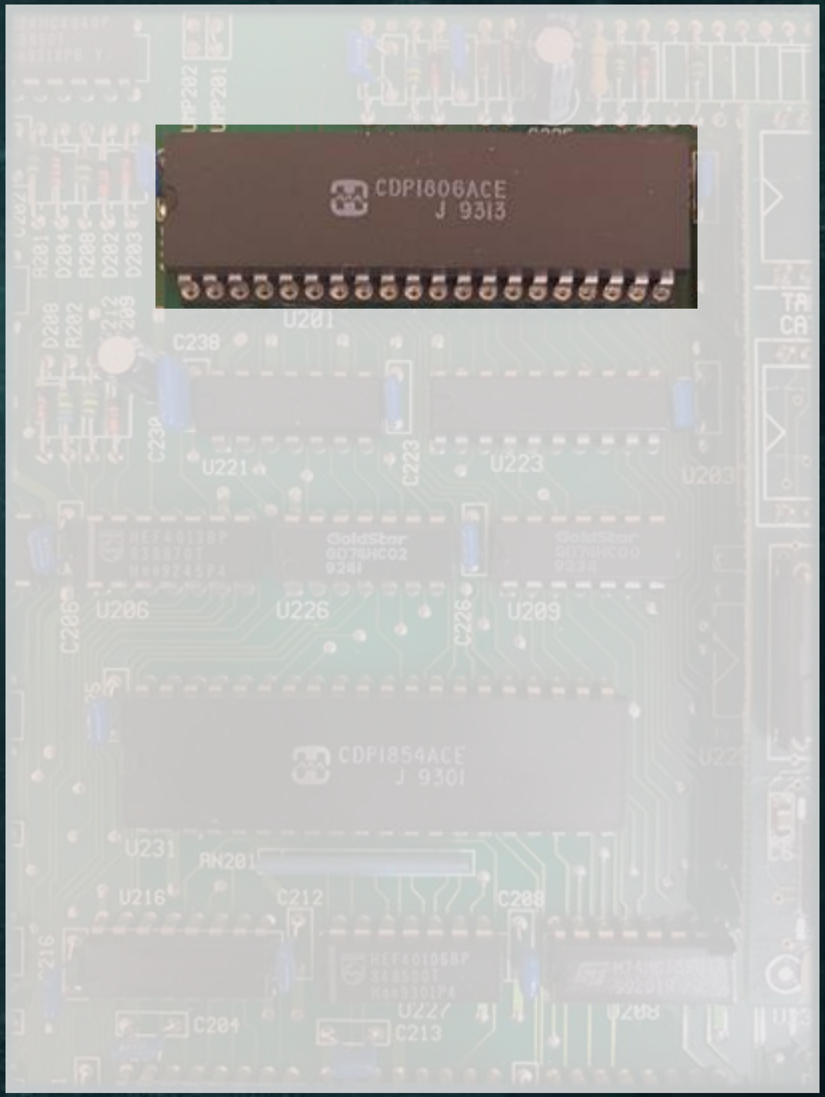
The processor design traces its history to an experimental home computer designed by Joseph Weisbecker in the early 1970s, built at his home using TTL components. RCA began development of the CMOS version of the processor design in 1973, sampling it in 1974 with plans to move to a single-chip implementation immediately. Jerry Herzog led the design of the single-chip version, which sampled in 1975 and entered production in 1976.[3][4]

Successors to the 1802 are the CDP1804, CDP1805, and CDP1806, which have an extended instruction set, other enhanced features (like on-chip RAM and ROM, and built-in timer), with some versions running at faster clock speeds, though not a significant speed difference. Some features are also lost, like the DMA auto-boot loader functionality. There are also some minor pin function changes, but the line continues to be produced in its original 40-pin dual in-line package (DIP) format.[when?]

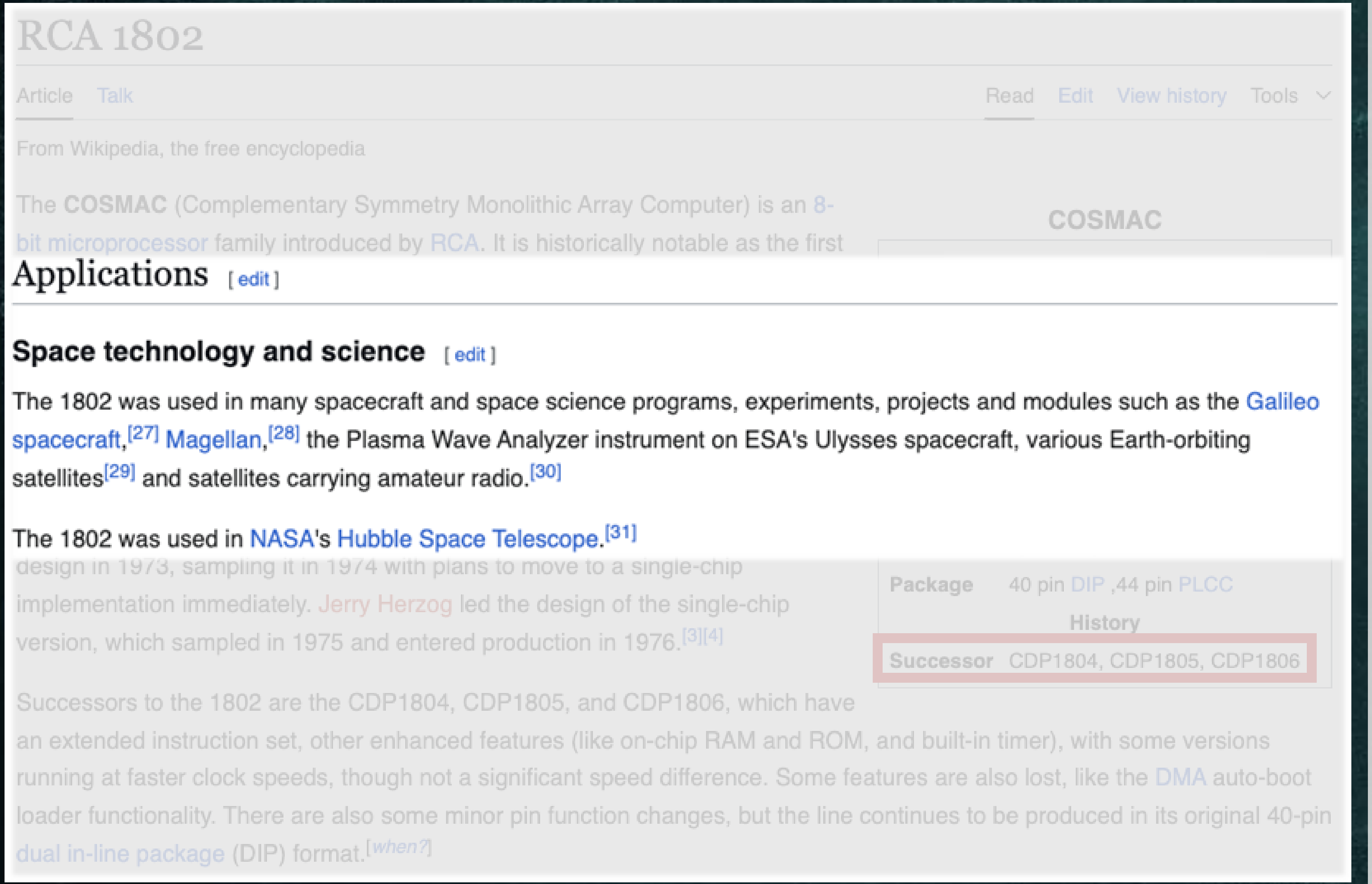
COSMAC

RCA CDP 1802

General information	
Launched	1974
Physical specifications	
Package	40 pin DIP ,44 pin PLCC
History	
Successor	CDP1804, CDP1805, CDP1806



CPU Identification



RCA 1802

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

The **COSMAC** (Complementary Symmetry Monolithic Array Computer) is an 8-bit microprocessor family introduced by RCA. It is historically notable as the first

COSMAC

Applications [edit]

Space technology and science [edit]

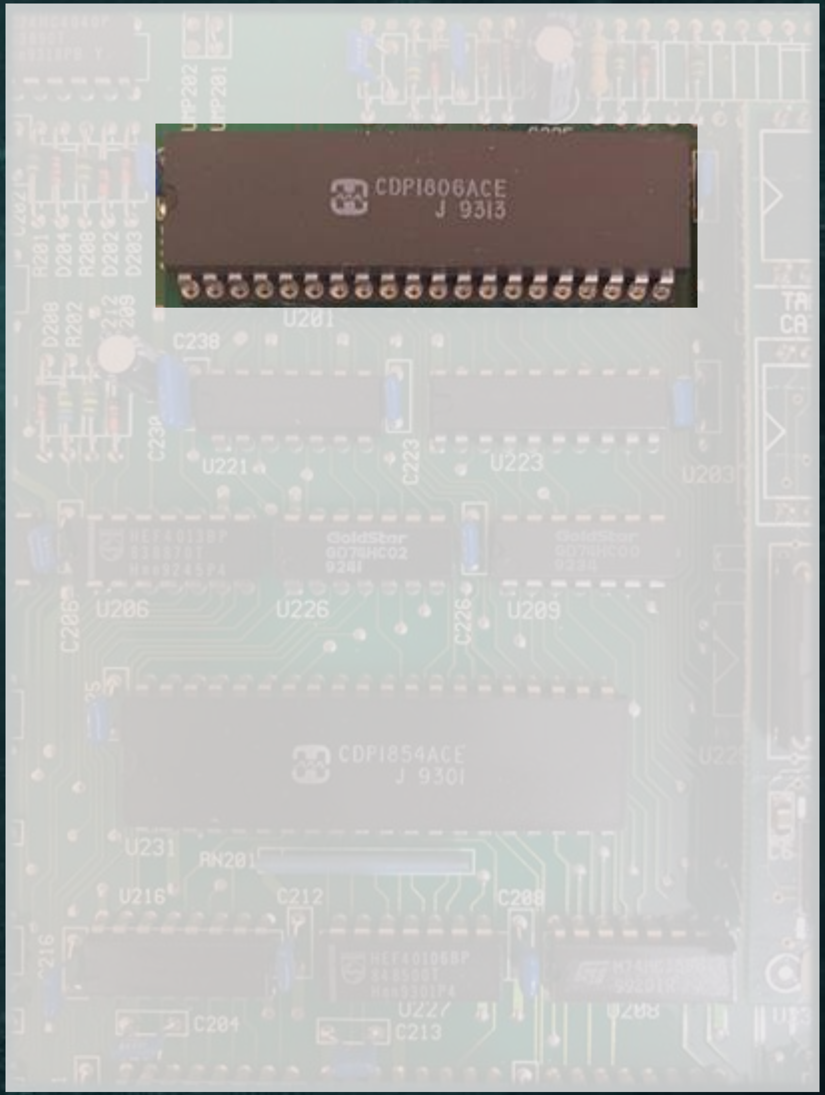
The 1802 was used in many spacecraft and space science programs, experiments, projects and modules such as the Galileo spacecraft,[27] Magellan,[28] the Plasma Wave Analyzer instrument on ESA's Ulysses spacecraft, various Earth-orbiting satellites[29] and satellites carrying amateur radio.[30]

The 1802 was used in NASA's Hubble Space Telescope.[31]

design in 1973, sampling it in 1974 with plans to move to a single-chip implementation immediately. Jerry Herzog led the design of the single-chip version, which sampled in 1975 and entered production in 1976.[3][4]

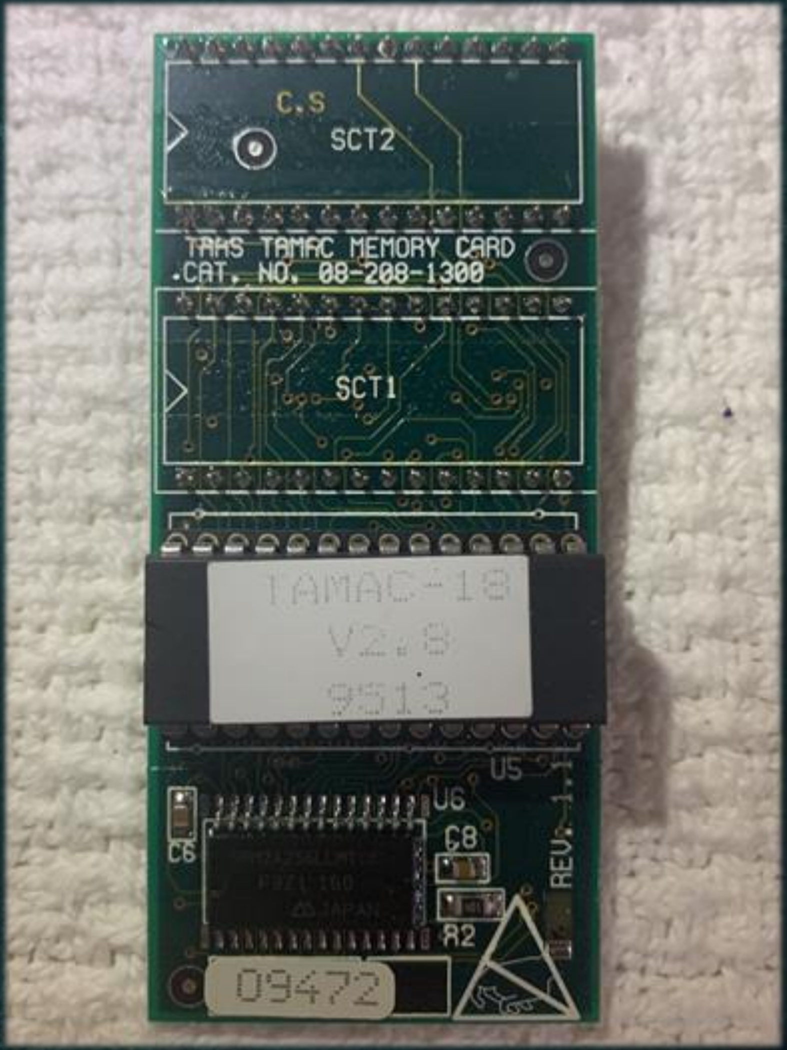
Package	40 pin DIP ,44 pin PLCC
History	
Successor	CDP1804, CDP1805, CDP1806

Successors to the 1802 are the CDP1804, CDP1805, and CDP1806, which have an extended instruction set, other enhanced features (like on-chip RAM and ROM, and built-in timer), with some versions running at faster clock speeds, though not a significant speed difference. Some features are also lost, like the DMA auto-boot loader functionality. There are also some minor pin function changes, but the line continues to be produced in its original 40-pin dual in-line package (DIP) format.[when?]



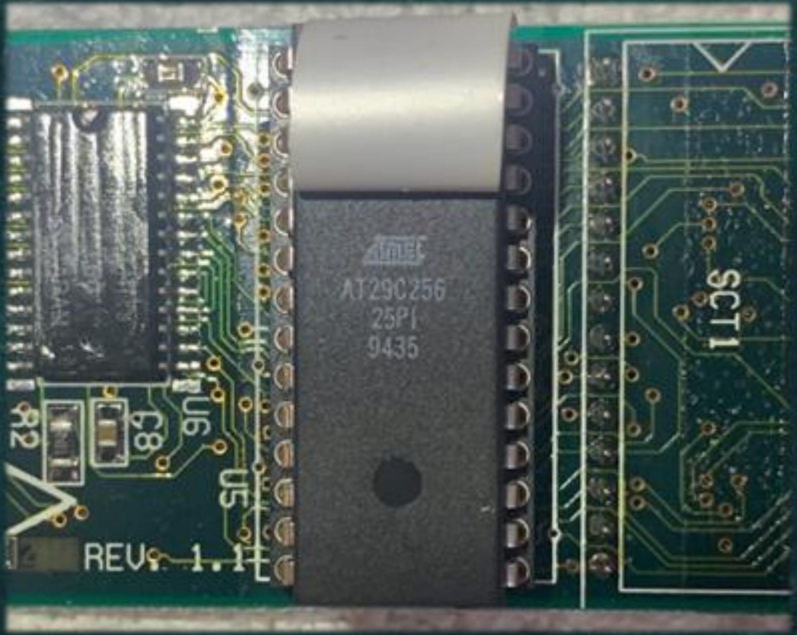
Firmware Extraction

- The firmware IC was easy to find.



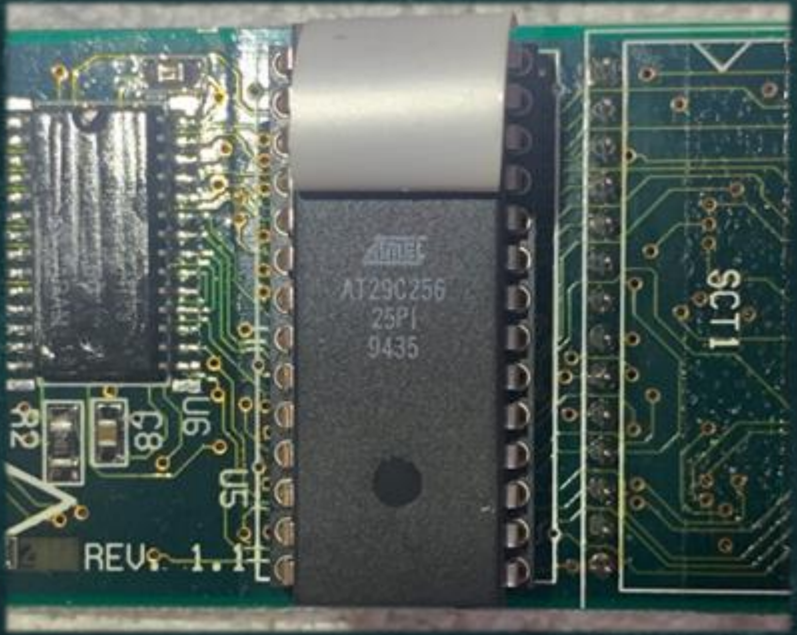
Firmware Extraction

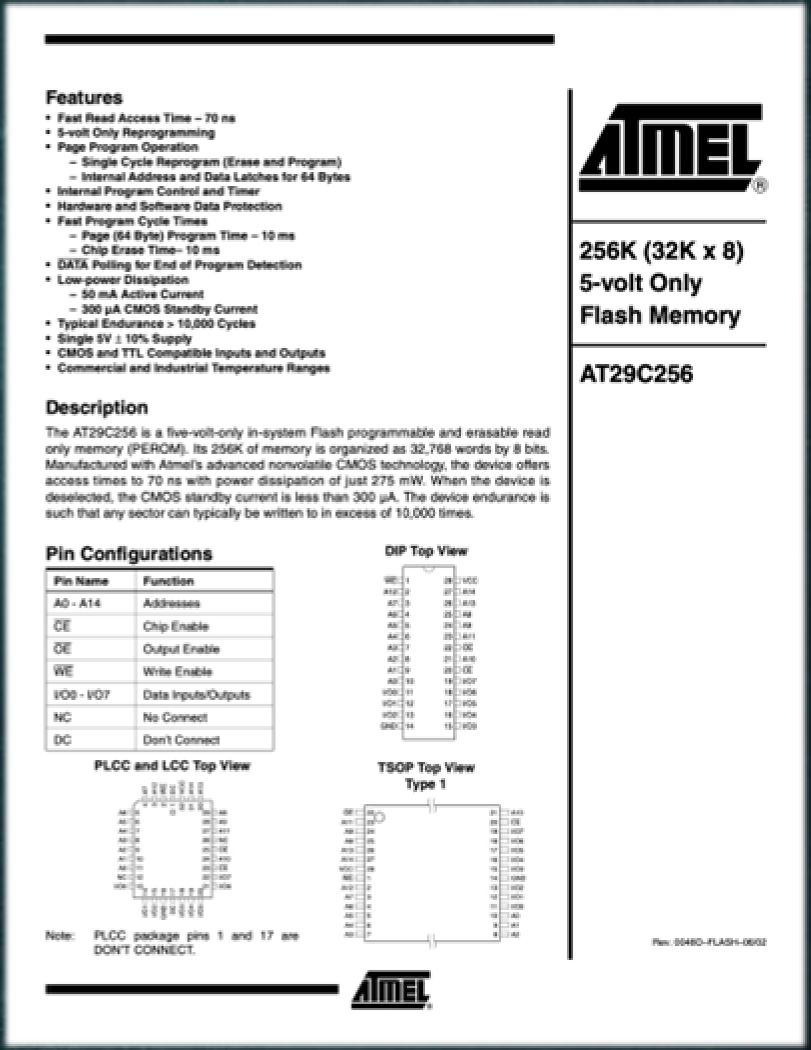
- The firmware IC was easy to find.
- It's an ATMEL AT29C256.



Firmware Extraction

- The firmware IC was easy to find.
- It's an ATMEL AT29C256.
  - 32KB





ATMEL

256K (32K x 8)
5-volt Only
Flash Memory

AT29C256

Features

- Fast Read Access Time – 70 ns
- 5-volt Only Reprogramming
- Page Program Operation
  - Single Cycle Reprogram (Erase and Program)
  - Internal Address and Data Latches for 64 Bytes
- Internal Program Control and Timer
- Hardware and Software Data Protection
- Fast Program Cycle Times
  - Page (64 Byte) Program Time – 10 ms
  - Chip Erase Time– 10 ms
- $\overline{\text{DATA}}$ Polling for End of Program Detection
- Low-power Dissipation
  - 50 mA Active Current
  - 300 µA CMOS Standby Current
- Typical Endurance > 10,000 Cycles
- Single 5V ± 10% Supply
- CMOS and TTL Compatible Inputs and Outputs
- Commercial and Industrial Temperature Ranges

Description

The AT29C256 is a five-volt-only in-system Flash programmable and erasable read only memory (PEROM). Its 256K of memory is organized as 32,768 words by 8 bits. Manufactured with Atmel's advanced nonvolatile CMOS technology, the device offers access times to 70 ns with power dissipation of just 275 mW. When the device is deselected, the CMOS standby current is less than 300 µA. The device endurance is such that any sector can typically be written to in excess of 10,000 times.

Pin Configurations

Pin Name	Function
A0 - A14	Addresses
$\overline{CE}$	Chip Enable
$\overline{OE}$	Output Enable
$\overline{WE}$	Write Enable
I/O0 - I/O7	Data Inputs/Outputs
NC	No Connect
DC	Don't Connect

DIP Top View

PLCC and LCC Top View

TSOP Top View
Type 1

Note: PLCC package pins 1 and 17 are DON'T CONNECT.

Rev. 0046O–FLASH–06/02

ATMEL

Firmware Extraction

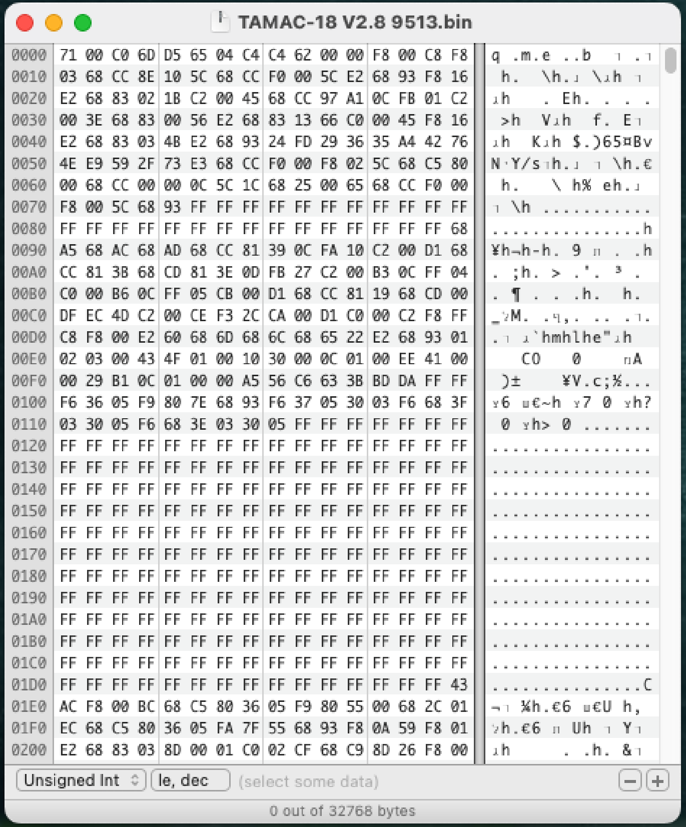
- Read the Flash

Firmware Extraction

- Read the Flash
  - There are better tools: TL866

Firmware Extraction

- Read the Flash
  - There are better tools: TL866
- Inspect the content

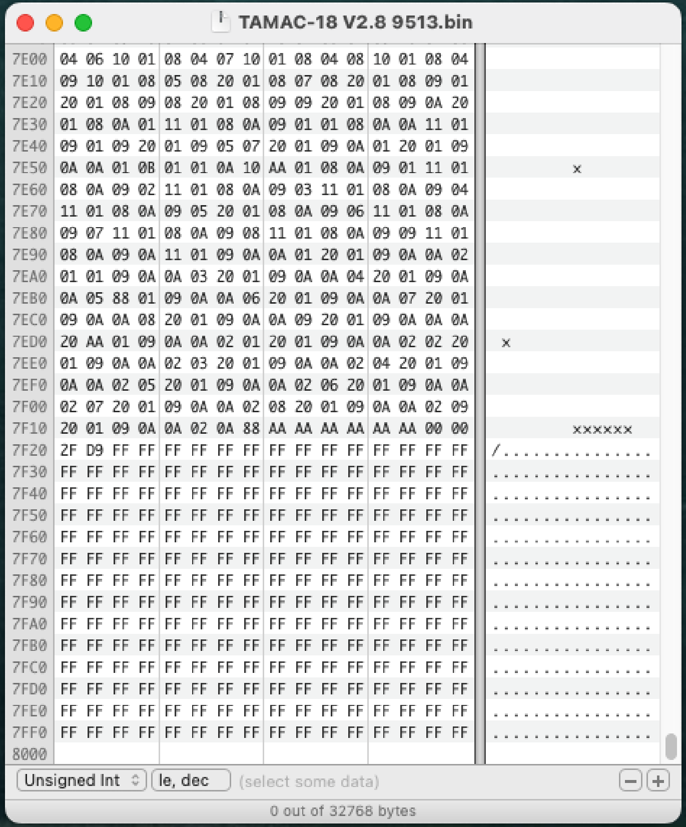


TAMAC-18 V2.8 9513.bin

```
0000  71 00 C0 6D D5 65 04 C4 C4 62 00 00 F8 00 C8 F8  q .m.e ..b  ┐ .┐
0010  03 68 CC 8E 10 5C 68 CC F0 00 5C E2 68 93 F8 16   h.  \h.ɹ \ɹh ┐
0020  E2 68 83 02 1B C2 00 45 68 CC 97 A1 0C FB 01 C2  ɹh   . Eh. . . .
0030  00 3E 68 83 00 56 E2 68 83 13 66 C0 00 45 F8 16   >h  Vɹh  f. E┐
0040  E2 68 83 03 4B E2 68 93 24 FD 29 36 35 A4 42 76  ɹh  Kɹh $.)65¤Bv
0050  4E E9 59 2F 73 E3 68 CC F0 00 F8 02 5C 68 C5 80  N·Y/s┐h.ɹ ┐ \h.€
0060  00 68 CC 00 00 0C 5C 1C 68 25 00 65 68 CC F0 00   h.   \ h% eh.ɹ
0070  F8 00 5C 68 93 FF FF FF FF FF FF FF FF FF FF FF  ┐ \h ...........
0080  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 68  ...............h
0090  A5 68 AC 68 AD 68 CC 81 39 0C FA 10 C2 00 D1 68  ¥h¬h-h. 9 ╥ . .h
00A0  CC 81 3B 68 CD 81 3E 0D FB 27 C2 00 B3 0C FF 04  . ;h. > .'. ³ .
00B0  C0 00 B6 0C FF 05 CB 00 D1 68 CC 81 19 68 CD 00  . ¶ . . .h.  h.
00C0  DF EC 4D C2 00 CE F3 2C CA 00 D1 C0 00 C2 F8 FF  _½M. .╕,. .. .┐.
00D0  C8 F8 00 E2 60 68 6D 68 6C 68 65 22 E2 68 93 01  .┐ ɹ`hmhlhe"ɹh
00E0  02 03 00 43 4F 01 00 10 30 00 0C 01 00 EE 41 00     CO    0    ╥A
00F0  00 29 B1 0C 01 00 00 A5 56 C6 63 3B BD DA FF FF   )±    ¥V.c;½...
0100  F6 36 05 F9 80 7E 68 93 F6 37 05 30 03 F6 68 3F  ɣ6 ╥€~h ɣ7 0 ɣh?
0110  03 30 05 F6 68 3E 03 30 05 FF FF FF FF FF FF FF   0 ɣh> 0 .......
0120  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
0130  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
0140  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
0150  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
0160  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
0170  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
0180  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
0190  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
01A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
01B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
01C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
01D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 43  ...............C
01E0  AC F8 00 BC 68 C5 80 36 05 F9 80 55 00 68 2C 01  ¬┐ ¼h.€6 ╥€U h,
01F0  EC 68 C5 80 36 05 FA 7F 55 68 93 F8 0A 59 F8 01  ½h.€6 ╥ Uh ┐ Y┐
0200  E2 68 83 03 8D 00 01 C0 02 CF 68 C9 8D 26 F8 00  ɹh     . .h. &┐
```

Unsigned Int | le, dec | (select some data)

0 out of 32768 bytes



TAMAC-18 V2.8 9513.bin

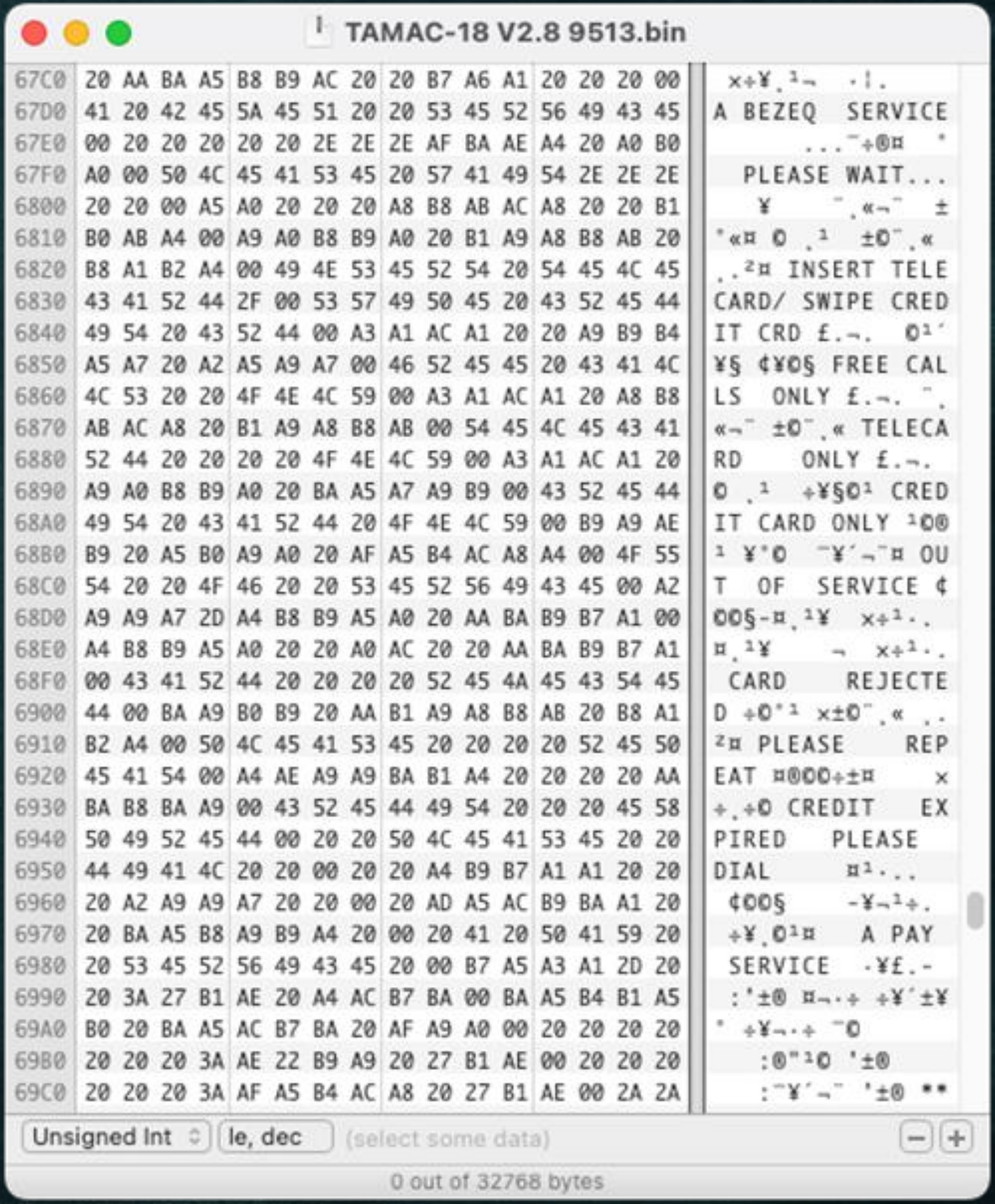
```
7E00  04 06 10 01 08 04 07 10 01 08 04 08 10 01 08 04
7E10  09 10 01 08 05 08 20 01 08 07 08 20 01 08 09 01
7E20  20 01 08 09 08 20 01 08 09 09 20 01 08 09 0A 20
7E30  01 08 0A 01 11 01 08 0A 09 01 01 08 0A 0A 11 01
7E40  09 01 09 20 01 09 05 07 20 01 09 0A 01 20 01 09
7E50  0A 0A 01 0B 01 01 0A 10 AA 01 08 0A 09 01 11 01          x
7E60  08 0A 09 02 11 01 08 0A 09 03 11 01 08 0A 09 04
7E70  11 01 08 0A 09 05 20 01 08 0A 09 06 11 01 08 0A
7E80  09 07 11 01 08 0A 09 08 11 01 08 0A 09 09 11 01
7E90  08 0A 09 0A 11 01 09 0A 0A 01 20 01 09 0A 0A 02
7EA0  01 01 09 0A 0A 03 20 01 09 0A 0A 04 20 01 09 0A
7EB0  0A 05 88 01 09 0A 0A 06 20 01 09 0A 0A 07 20 01
7EC0  09 0A 0A 08 20 01 09 0A 0A 09 20 01 09 0A 0A 0A
7ED0  20 AA 01 09 0A 0A 02 01 20 01 09 0A 0A 02 02 20   x
7EE0  01 09 0A 0A 02 03 20 01 09 0A 0A 02 04 20 01 09
7EF0  0A 0A 02 05 20 01 09 0A 0A 02 06 20 01 09 0A 0A
7F00  02 07 20 01 09 0A 0A 02 08 20 01 09 0A 0A 02 09
7F10  20 01 09 0A 0A 02 0A 88 AA AA AA AA AA AA 00 00          xxxxxx
7F20  2F D9 FF FF FF FF FF FF FF FF FF FF FF FF FF FF  /...............
7F30  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7F40  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7F50  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7F60  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7F70  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7F80  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7F90  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7FA0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7FB0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7FC0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7FD0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7FE0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7FF0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
8000
```

Unsigned Int | le, dec | (select some data)

0 out of 32768 bytes

Firmware Extraction

- Read the Flash
  - There are better tools: TL866
- Inspect the content
- Look for strings
  - Indictive strings



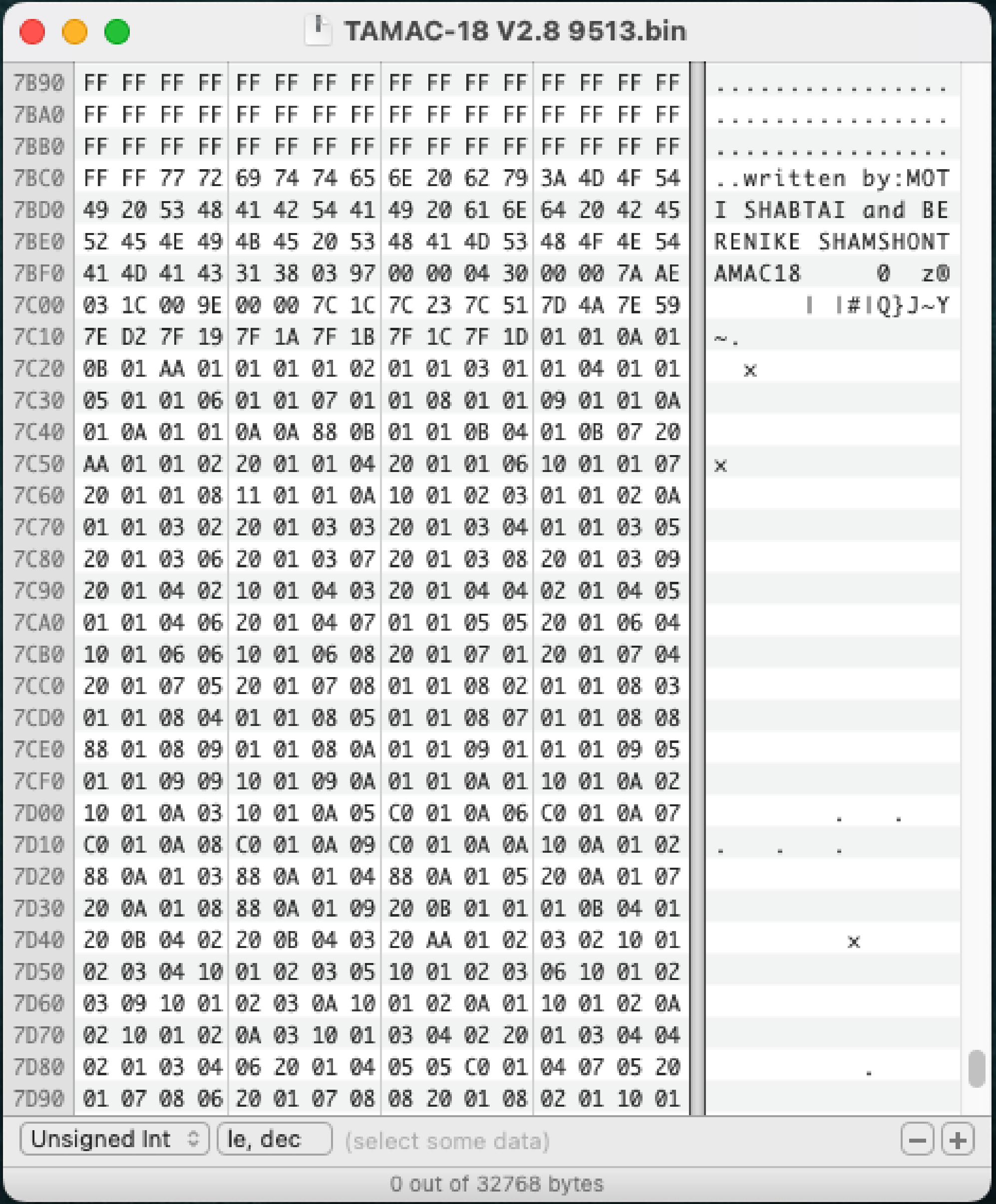
TAMAC-18 V2.8 9513.bin

```
67C0  20 AA BA A5 B8 B9 AC 20 20 B7 A6 A1 20 20 20 00   ×÷¥¸¹¬  ·¦.
67D0  41 20 42 45 5A 45 51 20 20 53 45 52 56 49 43 45  A BEZEQ  SERVICE
67E0  00 20 20 20 20 20 2E 2E 2E AF BA AE A4 20 A0 B0       ...¯÷®¤  °
67F0  A0 00 50 4C 45 41 53 45 20 57 41 49 54 2E 2E 2E    PLEASE WAIT...
6800  20 20 00 A5 A0 20 20 20 A8 B8 AB AC A8 20 20 B1     ¥    ¨¸«¬¨  ±
6810  B0 AB A4 00 A9 A0 B8 B9 A0 20 B1 A9 A8 B8 AB 20  °«¤ © ¸¹  ±©¨¸« 
6820  B8 A1 B2 A4 00 49 4E 53 45 52 54 20 54 45 4C 45  ¸¡²¤ INSERT TELE
6830  43 41 52 44 2F 00 53 57 49 50 45 20 43 52 45 44  CARD/ SWIPE CRED
6840  49 54 20 43 52 44 00 A3 A1 AC A1 20 20 A9 B9 B4  IT CRD £¡¬¡  ©¹´
6850  A5 A7 20 A2 A5 A9 A7 00 46 52 45 45 20 43 41 4C  ¥§ ¢¥©§ FREE CAL
6860  4C 53 20 20 4F 4E 4C 59 00 A3 A1 AC A1 20 A8 B8  LS  ONLY £¡¬¡ ¨¸
6870  AB AC A8 20 B1 A9 A8 B8 AB 00 54 45 4C 45 43 41  «¬¨ ±©¨¸« TELECA
6880  52 44 20 20 20 20 4F 4E 4C 59 00 A3 A1 AC A1 20  RD    ONLY £¡¬¡ 
6890  A9 A0 B8 B9 A0 20 BA A5 A7 A9 B9 00 43 52 45 44  © ¸¹  ÷¥§©¹ CRED
68A0  49 54 20 43 41 52 44 20 4F 4E 4C 59 00 B9 A9 AE  IT CARD ONLY ¹©®
68B0  B9 20 A5 B0 A9 A0 20 AF A5 B4 AC A8 A4 00 4F 55  ¹ ¥°©  ¯¥´¬¨¤ OU
68C0  54 20 20 4F 46 20 20 53 45 52 56 49 43 45 00 A2  T  OF  SERVICE ¢
68D0  A9 A9 A7 2D A4 B8 B9 A5 A0 20 AA BA B9 B7 A1 00  ©©§-¤¸¹¥  ×÷¹·¡
68E0  A4 B8 B9 A5 A0 20 20 A0 AC 20 20 AA BA B9 B7 A1  ¤¸¹¥    ¬  ×÷¹·¡
68F0  00 43 41 52 44 20 20 20 20 52 45 4A 45 43 54 45   CARD    REJECTE
6900  44 00 BA A9 B0 B9 20 AA B1 A9 A8 B8 AB 20 B8 A1  D ÷©°¹ ×±©¨¸« ¸¡
6910  B2 A4 00 50 4C 45 41 53 45 20 20 20 20 52 45 50  ²¤ PLEASE    REP
6920  45 41 54 00 A4 AE A9 A9 BA B1 A4 20 20 20 20 AA  EAT ¤®©©÷±¤    ×
6930  BA B8 BA A9 00 43 52 45 44 49 54 20 20 20 45 58  ÷¸÷© CREDIT   EX
6940  50 49 52 45 44 00 20 20 50 4C 45 41 53 45 20 20  PIRED   PLEASE  
6950  44 49 41 4C 20 20 00 20 20 A4 B9 B7 A1 A1 20 20  DIAL     ¤¹·¡¡  
6960  20 A2 A9 A9 A7 20 20 00 20 AD A5 AC B9 BA A1 20   ¢©©§    -¥¬¹÷¡ 
6970  20 BA A5 B8 A9 B9 A4 20 00 20 41 20 50 41 59 20   ÷¥¸©¹¤   A PAY 
6980  20 53 45 52 56 49 43 45 20 00 B7 A5 A3 A1 2D 20   SERVICE  ·¥£¡- 
6990  20 3A 27 B1 AE 20 A4 AC B7 BA 00 BA A5 B4 B1 A5   :'±® ¤¬·÷ ÷¥´±¥
69A0  B0 20 BA A5 AC B7 BA 20 AF A9 A0 00 20 20 20 20  ° ÷¥¬·÷ ¯©     
69B0  20 20 20 3A AE 22 B9 A9 20 27 B1 AE 00 20 20 20     :®"¹© '±®    
69C0  20 20 20 3A AF A5 B4 AC A8 20 27 B1 AE 00 2A 2A     :¯¥´¬¨ '±® **
```

0 out of 32768 bytes

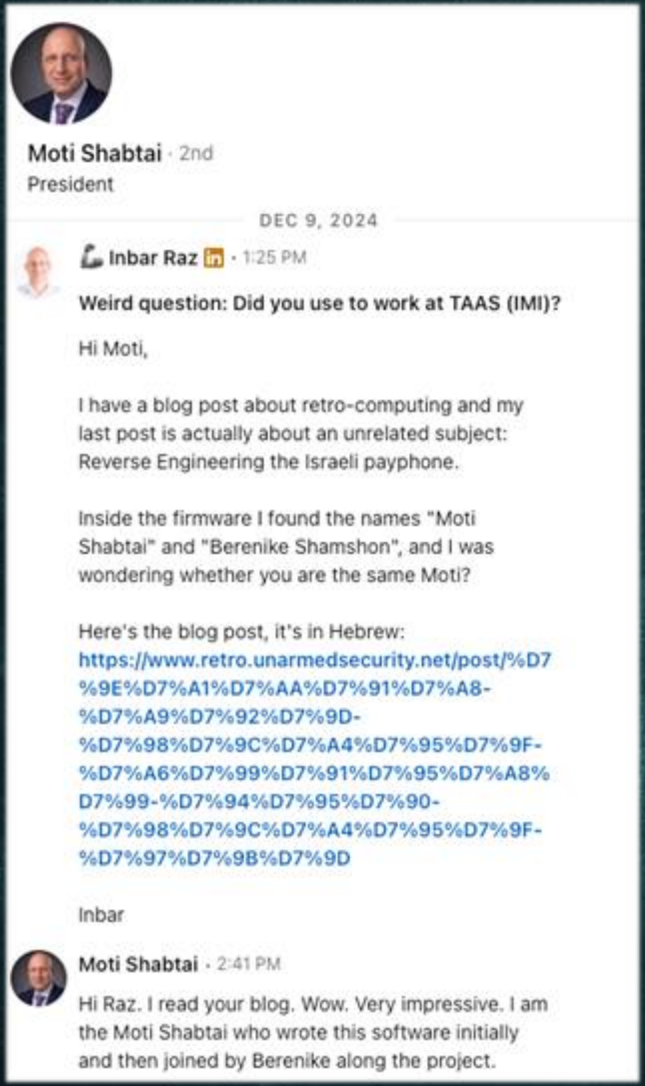
Firmware Extraction

- Read the Flash
  - There are better tools: TL866
- Inspect the content
- Look for strings
  - Indictive strings
  - Author names!



```
7B90  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7BA0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7BB0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
7BC0  FF FF 77 72 69 74 74 65 6E 20 62 79 3A 4D 4F 54  ..written by:MOT
7BD0  49 20 53 48 41 42 54 41 49 20 61 6E 64 20 42 45  I SHABTAI and BE
7BE0  52 45 4E 49 4B 45 20 53 48 41 4D 53 48 4F 4E 54  RENIKE SHAMSHONT
7BF0  41 4D 41 43 31 38 03 97 00 00 04 30 00 00 7A AE  AMAC18      0  z®
7C00  03 1C 00 9E 00 00 7C 1C 7C 23 7C 51 7D 4A 7E 59        |  |#|Q}J~Y
7C10  7E D2 7F 19 7F 1A 7F 1B 7F 1C 7F 1D 01 01 0A 01  ~.
7C20  0B 01 AA 01 01 01 01 02 01 01 03 01 01 04 01 01    ×
7C30  05 01 01 06 01 01 07 01 01 08 01 01 09 01 01 0A
7C40  01 0A 01 01 0A 0A 88 0B 01 01 0B 04 01 0B 07 20
7C50  AA 01 01 02 20 01 01 04 20 01 01 06 10 01 01 07  ×
7C60  20 01 01 08 11 01 01 0A 10 01 02 03 01 01 02 0A
7C70  01 01 03 02 20 01 03 03 20 01 03 04 01 01 03 05
7C80  20 01 03 06 20 01 03 07 20 01 03 08 20 01 03 09
7C90  20 01 04 02 10 01 04 03 20 01 04 04 02 01 04 05
7CA0  01 01 04 06 20 01 04 07 01 01 05 05 20 01 06 04
7CB0  10 01 06 06 10 01 06 08 20 01 07 01 20 01 07 04
7CC0  20 01 07 05 20 01 07 08 01 01 08 02 01 01 08 03
7CD0  01 01 08 04 01 01 08 05 01 01 08 07 01 01 08 08
7CE0  88 01 08 09 01 01 08 0A 01 01 09 01 01 01 09 05
7CF0  01 01 09 09 10 01 09 0A 01 01 0A 01 10 01 0A 02
7D00  10 01 0A 03 10 01 0A 05 C0 01 0A 06 C0 01 0A 07          .   .
7D10  C0 01 0A 08 C0 01 0A 09 C0 01 0A 0A 10 0A 01 02  .   .   .
7D20  88 0A 01 03 88 0A 01 04 88 0A 01 05 20 0A 01 07
7D30  20 0A 01 08 88 0A 01 09 20 0B 01 01 01 0B 04 01
7D40  20 0B 04 02 20 0B 04 03 20 AA 01 02 03 02 10 01           ×
7D50  02 03 04 10 01 02 03 05 10 01 02 03 06 10 01 02
7D60  03 09 10 01 02 03 0A 10 01 02 0A 01 10 01 02 0A
7D70  02 10 01 02 0A 03 10 01 03 04 02 20 01 03 04 04
7D80  02 01 03 04 06 20 01 04 05 05 C0 01 04 07 05 20            .
7D90  01 07 08 06 20 01 07 08 08 20 01 08 02 01 10 01
```

Moti Shabtai



Moti Shabtai · 2nd

President

DEC 9, 2024

Inbar Raz in · 1:25 PM

Weird question: Did you use to work at TAAS (IMI)?

Hi Moti,

I have a blog post about retro-computing and my last post is actually about an unrelated subject: Reverse Engineering the Israeli payphone.

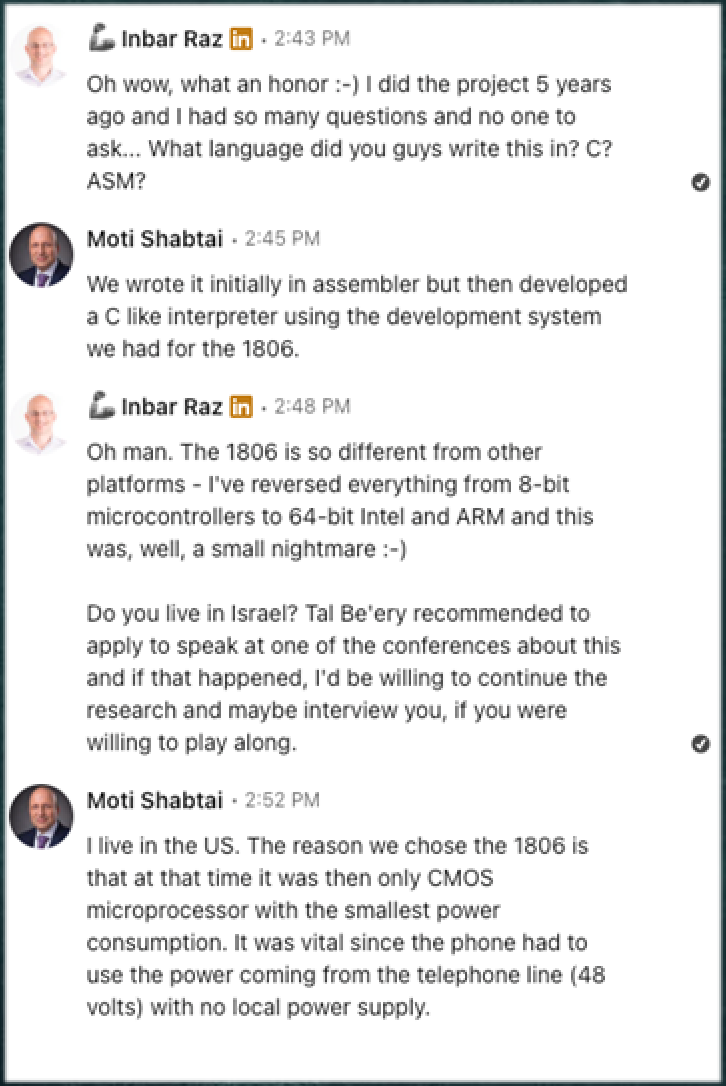
Inside the firmware I found the names "Moti Shabtai" and "Berenike Shamshon", and I was wondering whether you are the same Moti?

Here's the blog post, it's in Hebrew:
https://www.retro.unarmedsecurity.net/post/%D7%9E%D7%A1%D7%AA%D7%91%D7%A8-%D7%A9%D7%92%D7%9D-%D7%98%D7%9C%D7%A4%D7%95%D7%9F-%D7%A6%D7%99%D7%91%D7%95%D7%A8%D7%99-%D7%94%D7%95%D7%90-%D7%98%D7%9C%D7%A4%D7%95%D7%9F-%D7%97%D7%9B%D7%9D

Inbar

Moti Shabtai · 2:41 PM

Hi Raz. I read your blog. Wow. Very impressive. I am the Moti Shabtai who wrote this software initially and then joined by Berenike along the project.



Inbar Raz in · 2:43 PM

Oh wow, what an honor :-) I did the project 5 years ago and I had so many questions and no one to ask... What language did you guys write this in? C? ASM?

Moti Shabtai · 2:45 PM

We wrote it initially in assembler but then developed a C like interpreter using the development system we had for the 1806.

Inbar Raz in · 2:48 PM

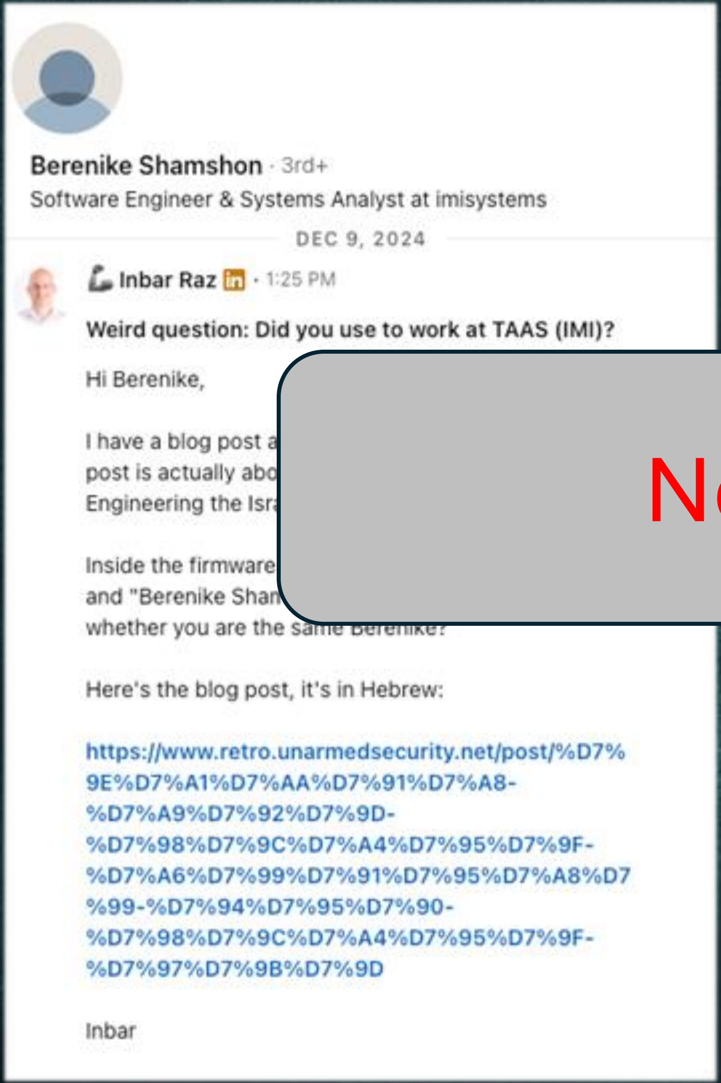
Oh man. The 1806 is so different from other platforms - I've reversed everything from 8-bit microcontrollers to 64-bit Intel and ARM and this was, well, a small nightmare :-)

Do you live in Israel? Tal Be'ery recommended to apply to speak at one of the conferences about this and if that happened, I'd be willing to continue the research and maybe interview you, if you were willing to play along.

Moti Shabtai · 2:52 PM

I live in the US. The reason we chose the 1806 is that at that time it was then only CMOS microprocessor with the smallest power consumption. It was vital since the phone had to use the power coming from the telephone line (48 volts) with no local power supply.

Berenike Shamshon



Berenike Shamshon · 3rd+
Software Engineer & Systems Analyst at imisystems

DEC 9, 2024

Inbar Raz · 1:25 PM

Weird question: Did you use to work at TAAS (IMI)?

Hi Berenike,

I have a blog post a
post is actually abo
Engineering the Isra

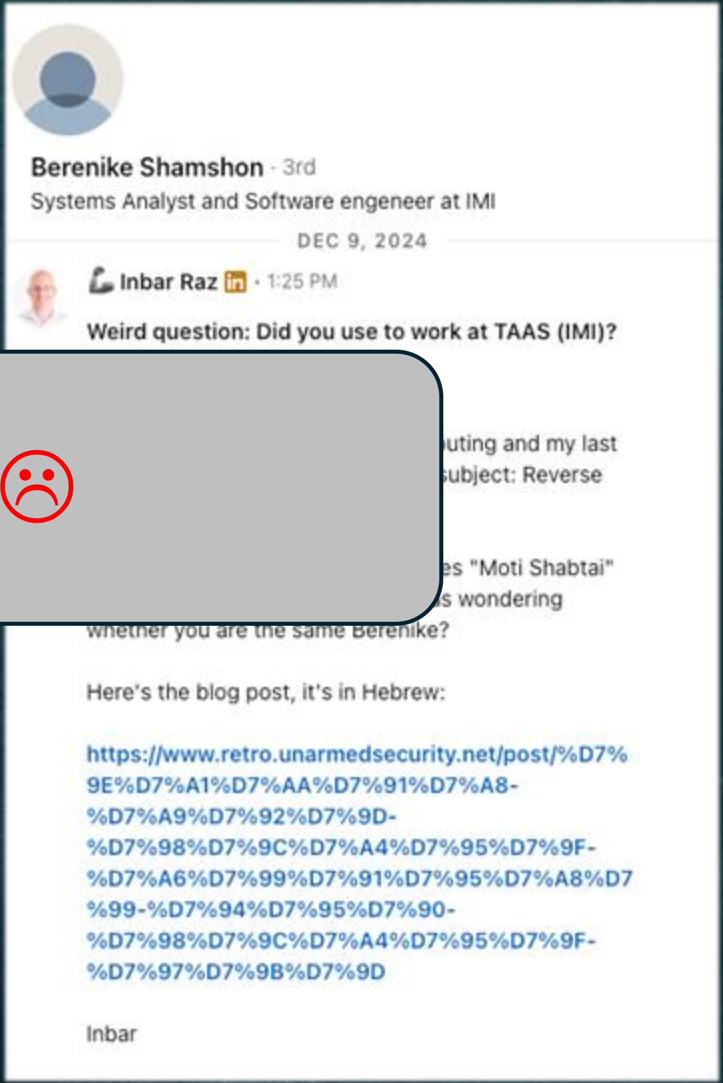
Inside the firmware
and "Berenike Shan
whether you are the same Berenike?

Here's the blog post, it's in Hebrew:

https://www.retro.unarmedsecurity.net/post/%D7%9E%D7%A1%D7%AA%D7%91%D7%A8-%D7%A9%D7%92%D7%9D-%D7%98%D7%9C%D7%A4%D7%95%D7%9F-%D7%A6%D7%99%D7%91%D7%95%D7%A8%D7%99-%D7%94%D7%95%D7%90-%D7%98%D7%9C%D7%A4%D7%95%D7%9F-%D7%97%D7%9B%D7%9D

Inbar

No luck ☹



Berenike Shamshon · 3rd
Systems Analyst and Software engeneer at IMI

DEC 9, 2024

Inbar Raz · 1:25 PM

Weird question: Did you use to work at TAAS (IMI)?

uting and my last
subject: Reverse

es "Moti Shabtai"
s wondering
whether you are the same Berenike?

Here's the blog post, it's in Hebrew:

https://www.retro.unarmedsecurity.net/post/%D7%9E%D7%A1%D7%AA%D7%91%D7%A8-%D7%A9%D7%92%D7%9D-%D7%98%D7%9C%D7%A4%D7%95%D7%9F-%D7%A6%D7%99%D7%91%D7%95%D7%A8%D7%99-%D7%94%D7%95%D7%90-%D7%98%D7%9C%D7%A4%D7%95%D7%9F-%D7%97%D7%9B%D7%9D

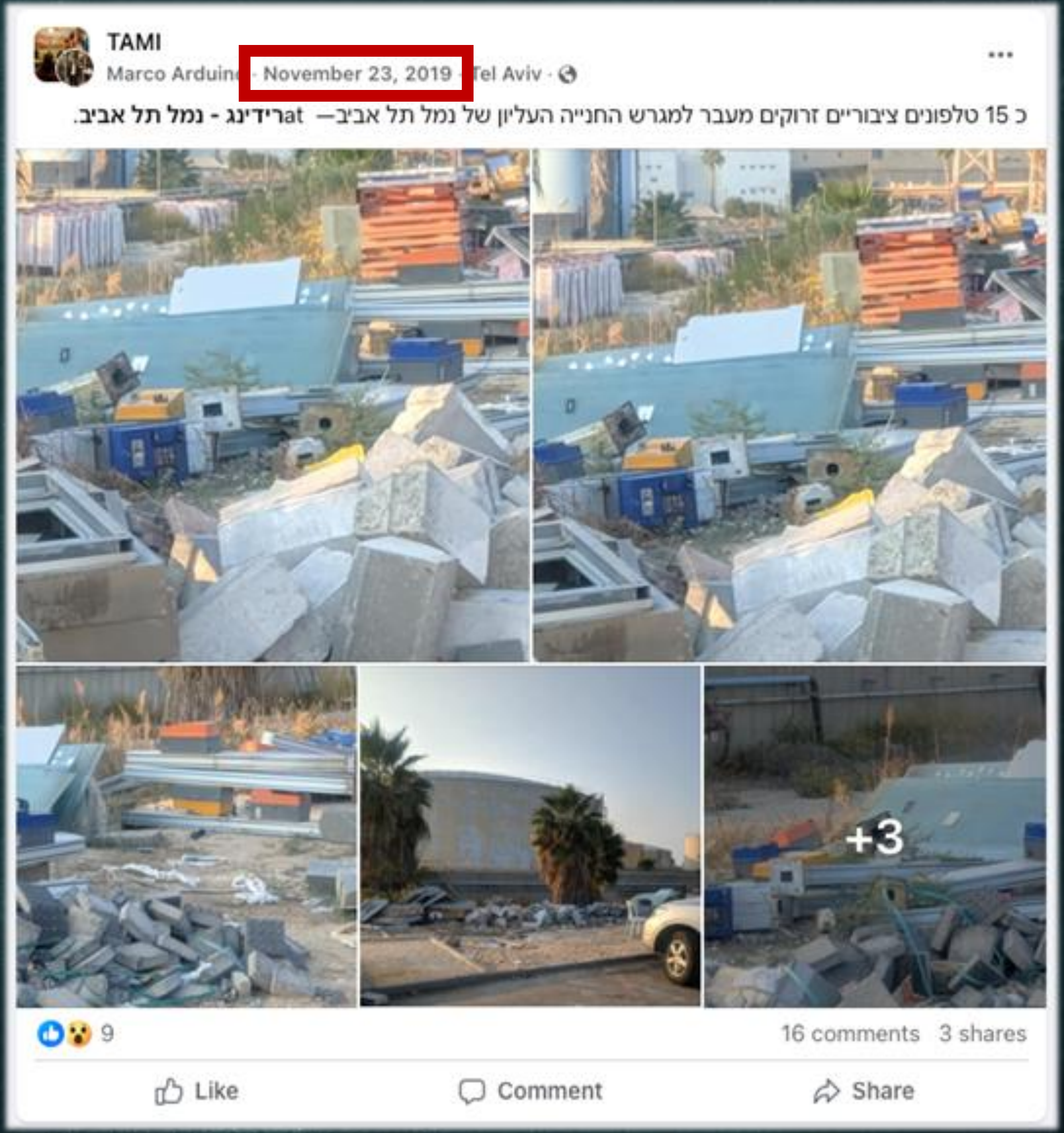
Inbar

TA0008:

Lateral Movement

Scaling up

- Hitting the Jackpot!
- Payphones were being dismantled and dumped.
- Pity and compassion took over.
  - Probably opportunism, too.



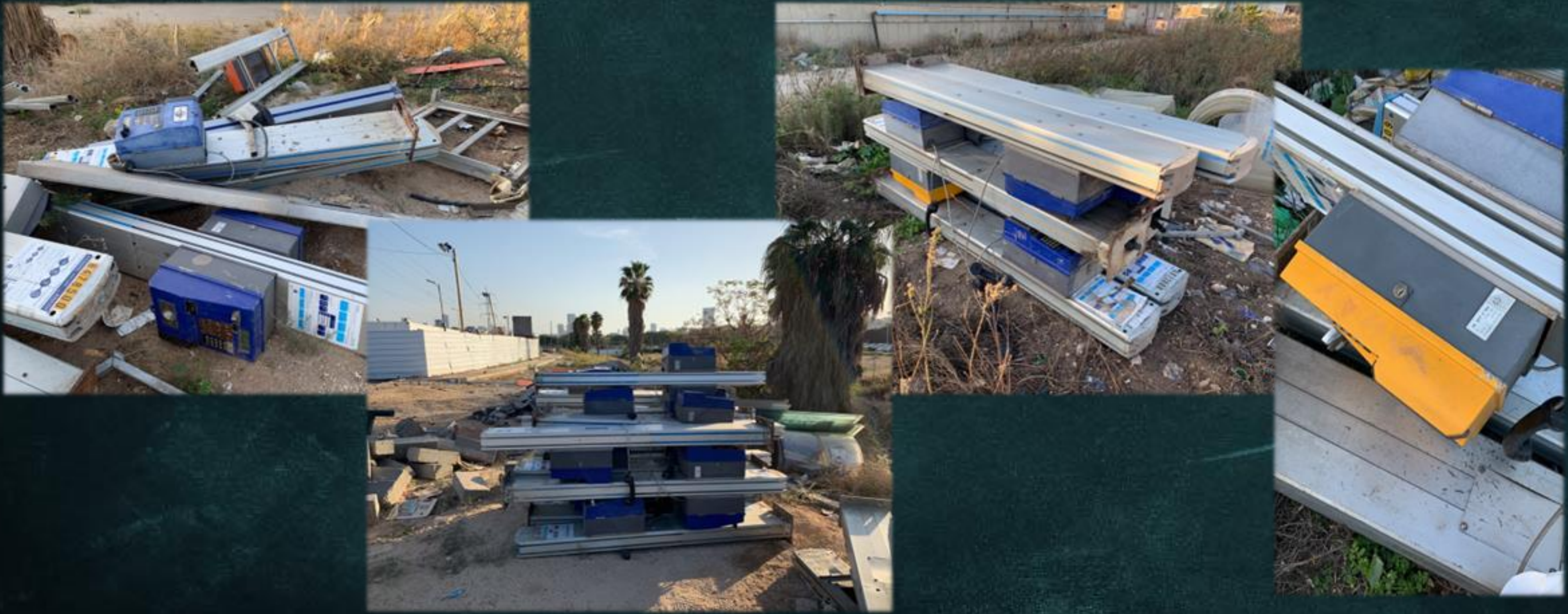
TAMI

Marco Arduin[illegible] · November 23, 2019 · Tel Aviv ·

כ 15 טלפונים ציבוריים זרוקים מעבר למגרש החנייה העליון של נמל תל אביב — at **רידינג - נמל תל אביב**.

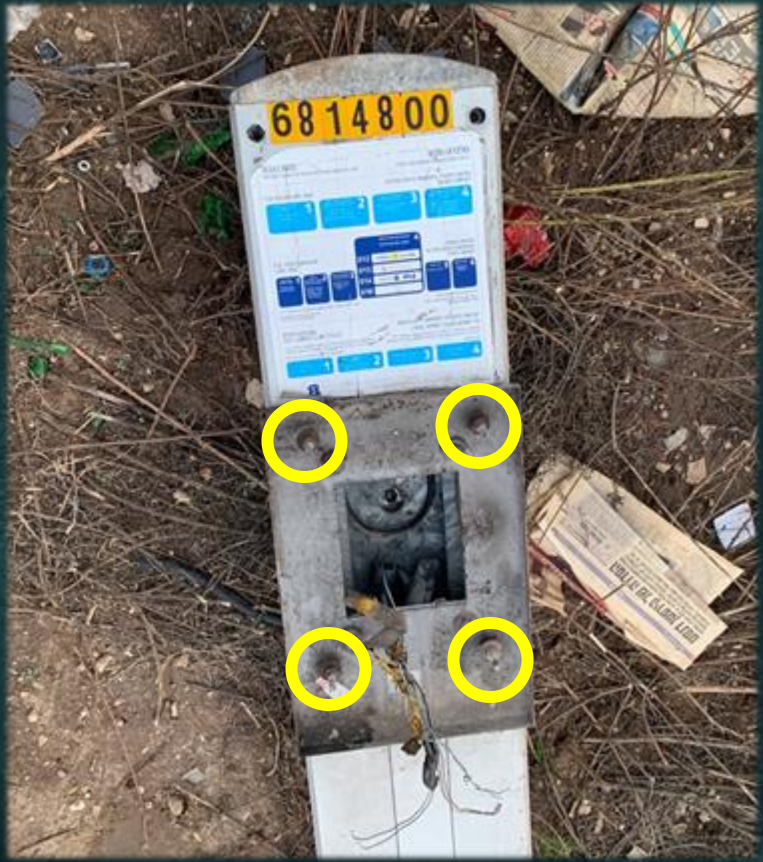
Hitting a snag

- Almost all phones were attached to poles.



Hitting a snag

- Almost all phones were attached to poles.
- The mounting bolts are inside the chassis.



Hitting a snag

- Almost all phones were attached to poles.
- The mounting bolts are inside the chassis.
- Lockpicking is no longer viable.

When the going gets tough...

Easier said than done...

- Some went easy.

Easier said than done…

- Some went easy.
- Some not so much…