Using a Microscope to Examine Integrated Circuits

Andrew Menadue, UK

Many years ago I accidentally sent far too many electrons through an integrated circuit I was working with. I can't remember the details, but I do remember the escape of the 'magic smoke'. In place of the integrated circuit I had soldered on to the board was a sooty mess. There was an upside to this incident, though, as the protective packaging of the integrated circuit had been turned from a tough resin type material to a more powdery consistency. It was easy to pick the packaging away and find the silicon gem inside. Gem is the correct word too, as the microscopic features on these silicon chips cause them to glint in various colurs if sunlight is allowed to reflect off them.

Rolling forward a few years and I realised that metallurgical microscopes allow a degree of reverse engineering of integrated circuits that I could find useful, so I bought an Olympus BHM. After making a few additions I had a microscope that could image the features on these devices. I won't go into the details of the microscope here, instead I want to outline how I get photographs of the internals and give an example of how this can be useful for reverse engineering.

Sourcing Dies

Getting hold of dies is relatively simple, as there's a lot of old electronics floating around. It's worth bearing in mind that the newer the electronics is, the more dense the features will be. Modern integrated circuits are now packed with features so small that to perform practical detailed reverse engineering requires an electron microscope rather than an optical microscope. These devices will provide interesting subjects for viewing alone, however. The sheer complexity of these devices can be astounding. Simpler devices can also be imaged, such as logic devices and transistors. Even modern versions of these devices can be studied with an optical microscope successfully due to the much simpler circuitry inolved. My interests are in fault determination, and reverse engineering vintage devices, so I find old equipment, preferably in a non-working state and depackage any devices I find inside.

Depackaging the Die

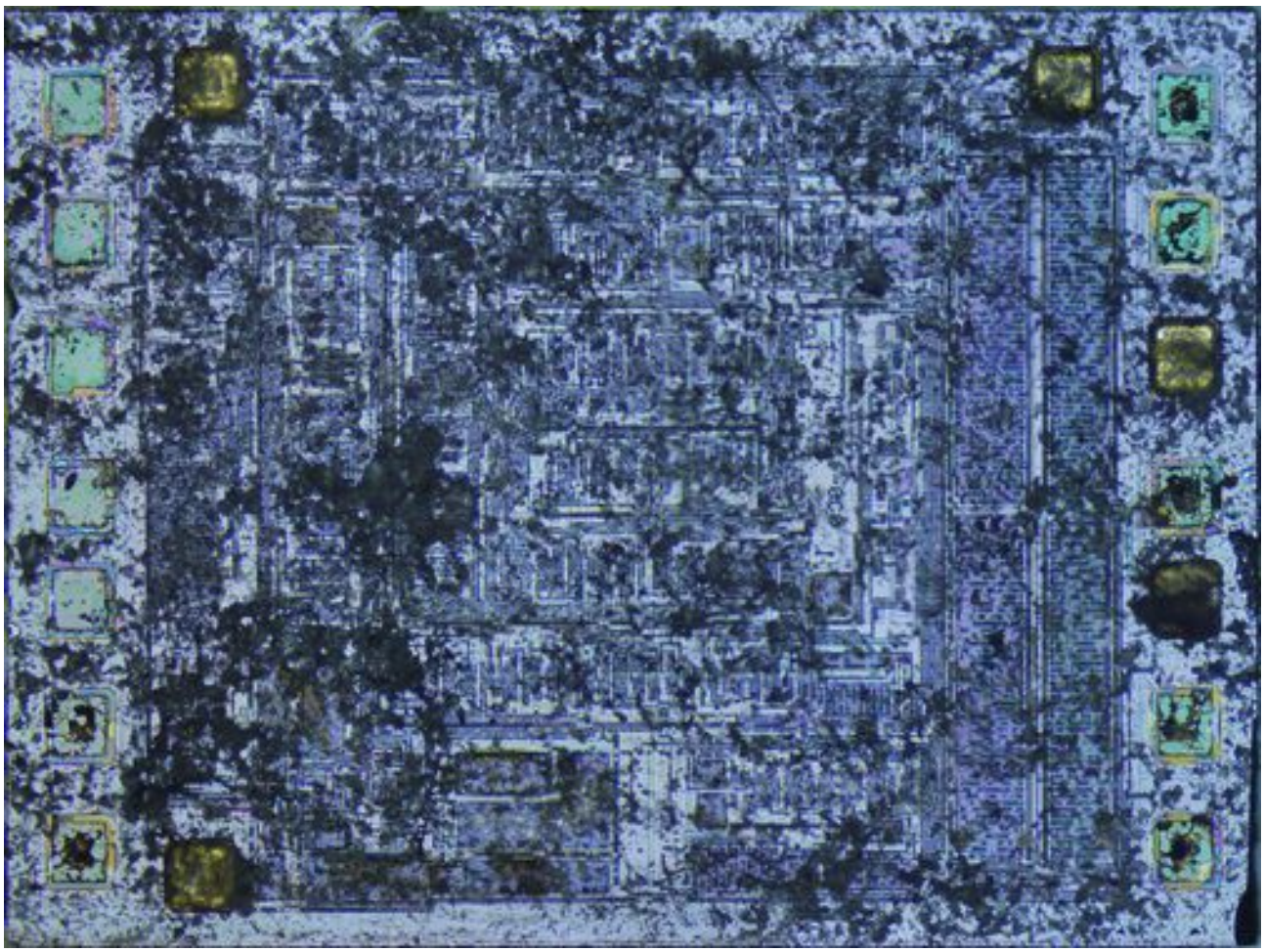
There are many people around the world who extract the 'dies' as the silicon chips are called from the protective packages. A lot of the methods use noxious chemicals such as nitric or hydrofluoric acid. These are not pleasant substances to use and can be quite dangerous. I decided to use a method that emulates the failed integrated circuit scenario I described above . Rather than using heat generated by a failed device, I use a small butane torch to heat the packages to the point at which they catch alight. A few seconds later and the device package usually turns to carbons and soot. Using needle nosed pliers I then gently pull the package apart. The legs are removed and the die extracted, hopefully without much damage. Sometimes the die is chipped or more rarely, broken into parts. This usually doesn't affect reverse engineering the device too much. Be careful when manipulating these dies with tweezers, as if they are held too strongly they tend to shoot off in some random direction or other. These dies are at most a few millimetres square and once dropped on the floor they seem to evaporate and never be seen again.

Different devices have different characteristics and some separate from the packaging easily, some take a bit more work. Now and again there seem to be coatings on dies and I may have to burn this off with a second heating with the torch. If there's a lot of debris on the die after removal from the package I use an ultrasonic cleaner to remove it. I use plain water as the cleaning fluid and run the cleaner for about 3 minutes.

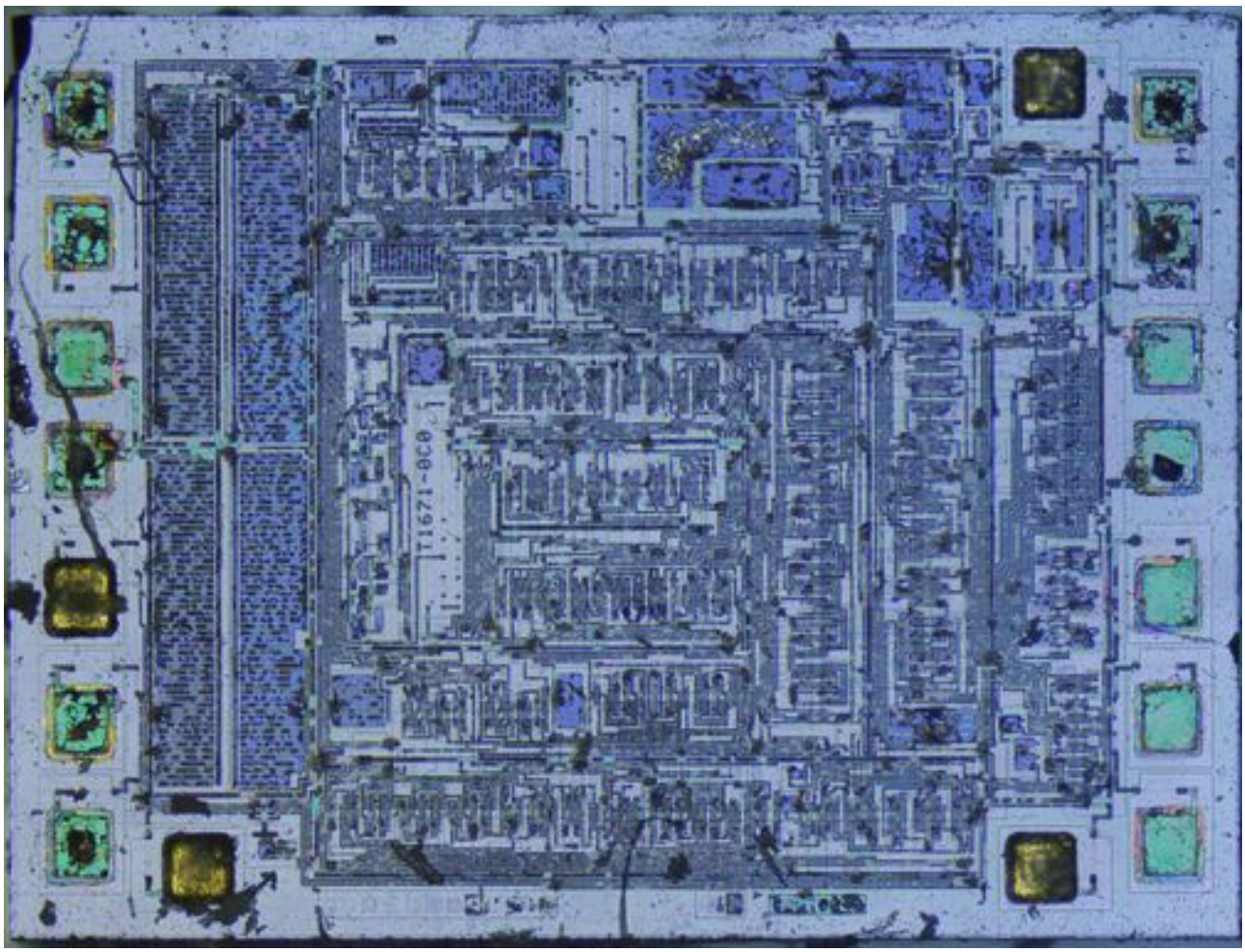
Imaging the Silicon

I use an Olympus BHM microscope to look at these dies, this is one of the uses it is designed for. Dies have thin layers of metal and doped silicon and sometimes the colours that appear under the microscope are intense. In order to more easily examine the die, I stitch together a grid of photographs of the die. I use a Panasonic GF1 micro four thirds camera for this, together with a camera mount tube that I made that fits on the top camera port of the trinocular head of the BHM. Depending on the size of the die and the magnification I am using the number of photographs I stitch can be as few as 10 or so, up to over two hundred. I use a program called 'hugin' to perform the stitching and run it on a fairly powerful machine. A large stitch process can still take several hours to stitch together.

This is a scaled down image of a die from a quartz watch, I've scaled it from the original which is 63Mb simply for practical reasons. Using the full size image I can move around the full die and zoom in to a high level of detail to examine circuitry. This image is of a die that has just been exposed to the torch flame. The black marks on the die are carbonised packaging remnants.



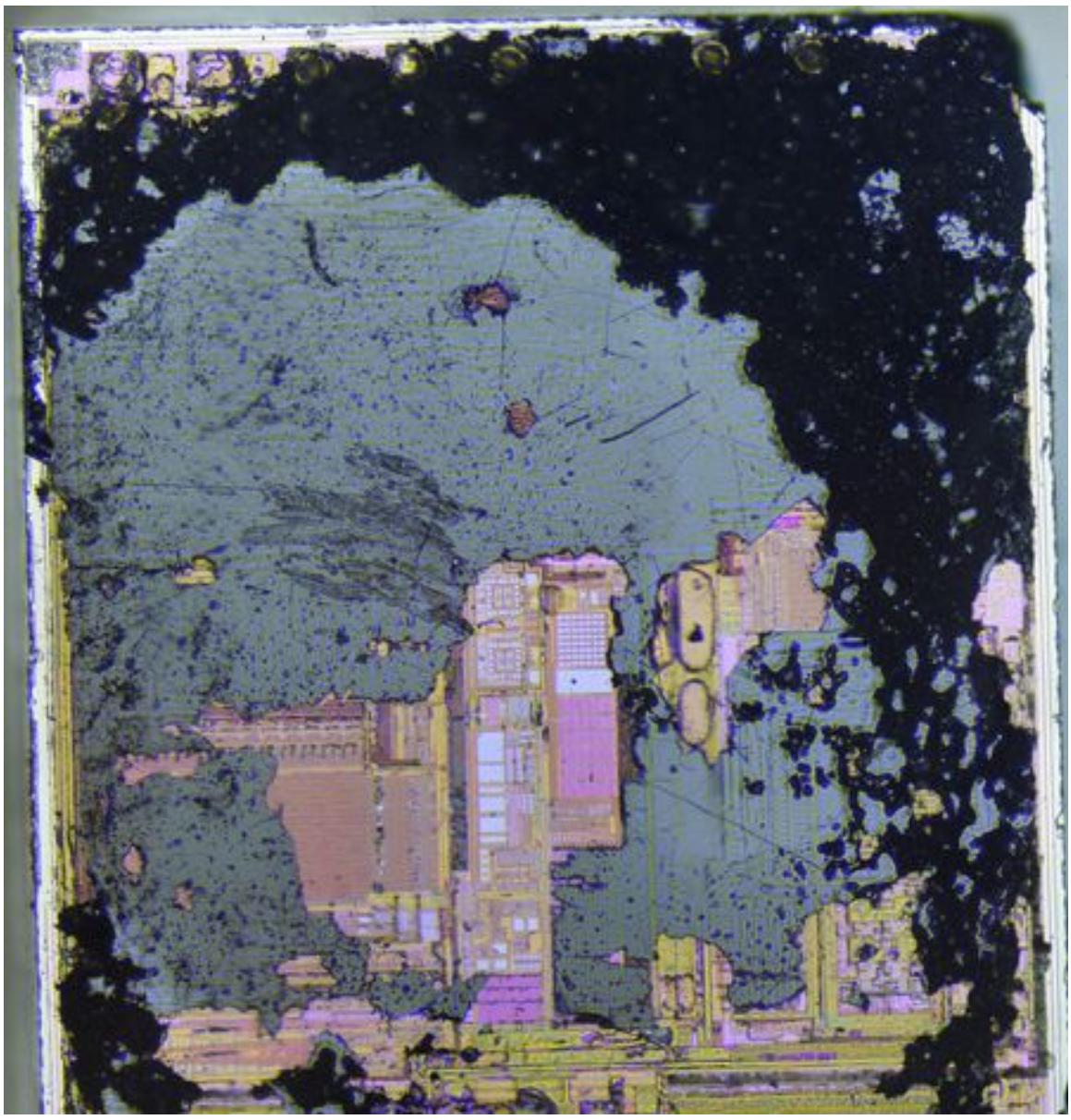
The next image is the same die after three minutes of ultrasonic cleaning. As can be seen, this is effective at removing carbonised material.



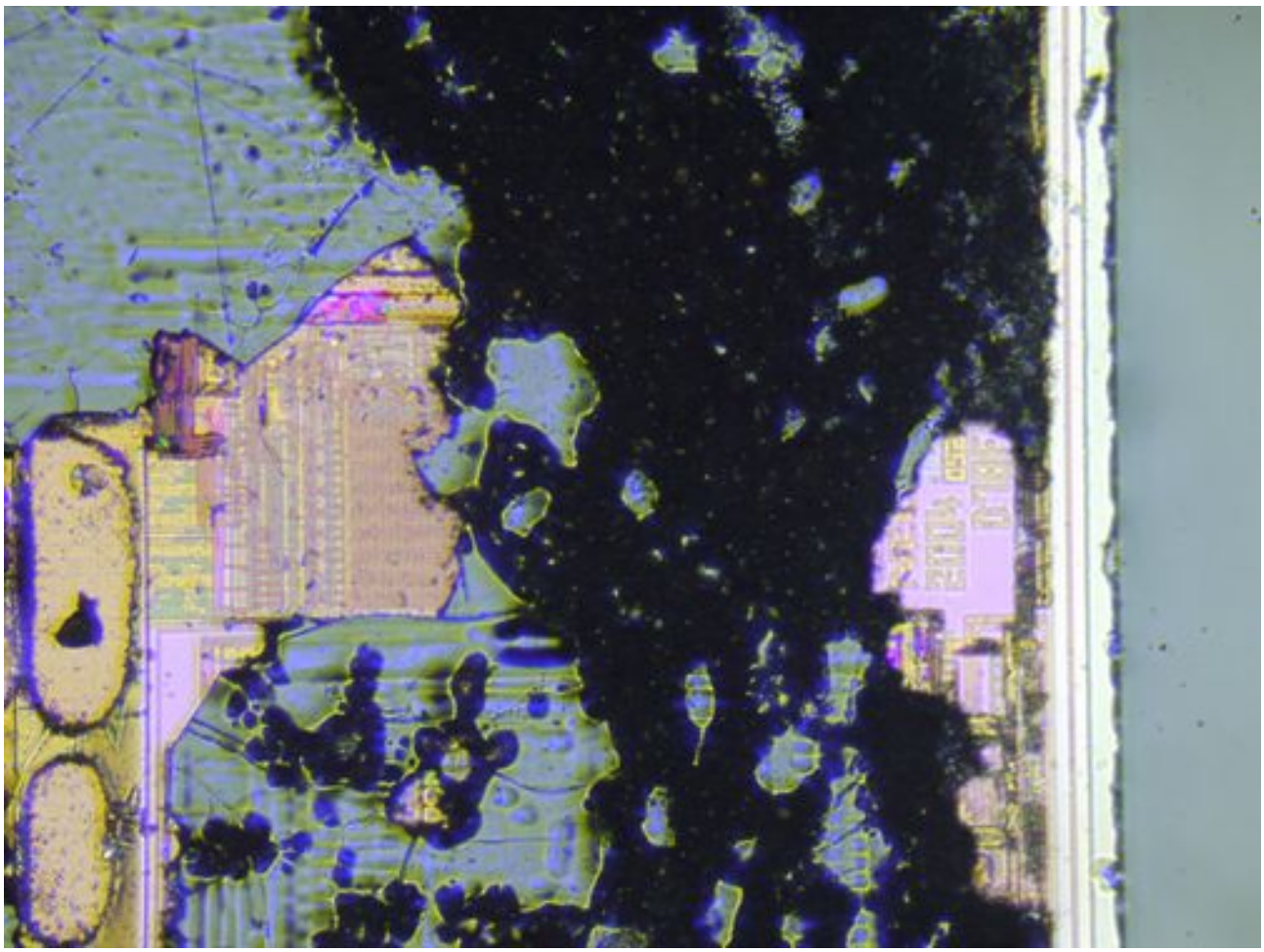
This is a fairly colourful die, and is quite simple, due to the functions required of a quartz watch not being too elaborate.

An Example

As an example of what can be done with reverse engineering, I recently dismantled a capsule coffee machine. This type of machine has various different capsules of flavoured coffee or milk that are processed in different ways by the machine. Depending on the drink that is required various different timings of water delivery and heating are created. This is all quite complex and requires the use of a microcontroller to handle all the timings and control of pumps and solenoids. One of the parts that I found in the machine was a circuit board that contained the microcontroller. I was quite interested in this PCB as microcontrollers can sometimes be reprogrammed and if so then the circuit board can be re-purposed. In this case the microcontroller package identification had been removed. This is fairly common and is probably used to prevent copying of the circuit by anyone who wanted to create cheap clones of the machine. As the identification of the microcontroller was missing, I had no way to determine what the features of the device were, and no way to program it. The device packages are standard, so the microcontroller could have been one of many types. Using the process detailed above, I removed the microcontroller, decapsulated the device and created a ‘die shot’ from a panorama of several photographs. The full die shot is about 45Mb in size. A reduced file size photograph is reproduced here:



This device is one that has some sort of coating on top of the die, this is that darker black and grey areas in the photo. If I want a better view of the die, I'd try to remove this coating by burning it off and then attempting to clean the remains in an ultrasonic cleaner. In this case the die has given up enough of its secrets. In the middle of the right hand side we see this:



In the cleared area to the right you can see ‘NEC’ and D78F. This is enough to identify the device as an NEC UPD78F series microcontroller. The number of pins on the PCB that the package has narrows down the exact variation of that microcontroller. If I want to re-use the PCB I can find some devices that fit on the PCB and program them as required. A PCB that was scrap is now reusable, with a bit of work.

Gallery

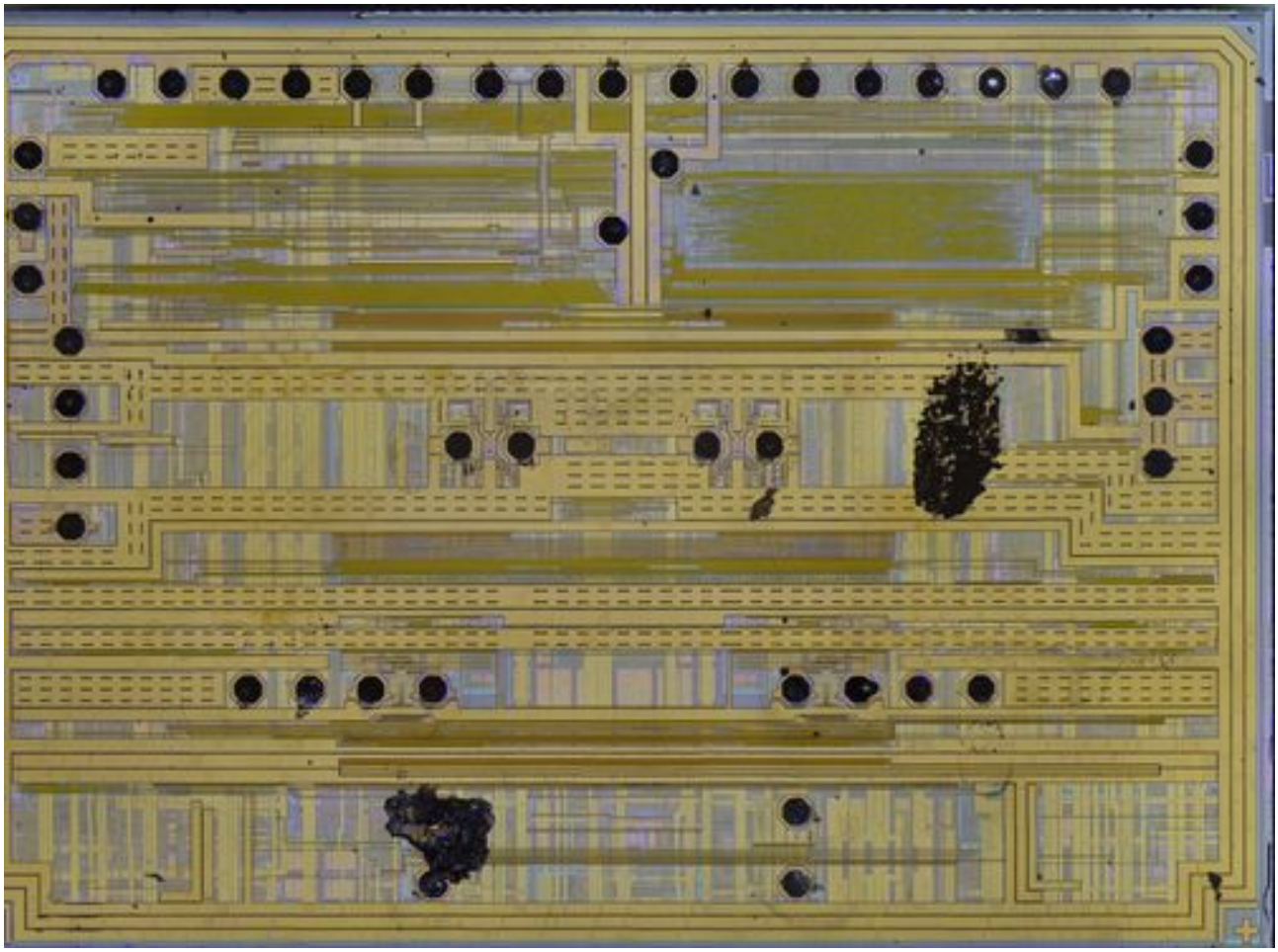
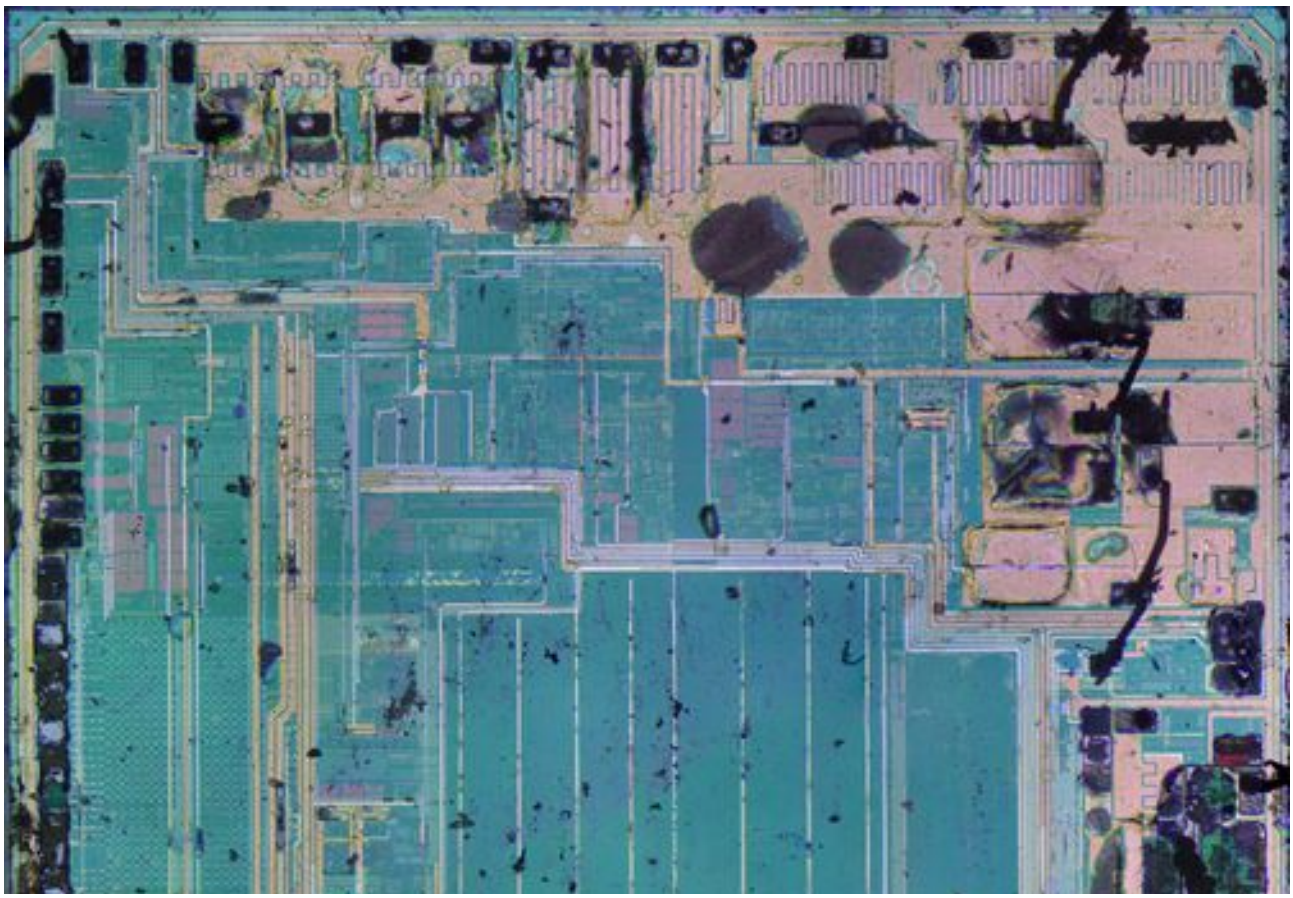
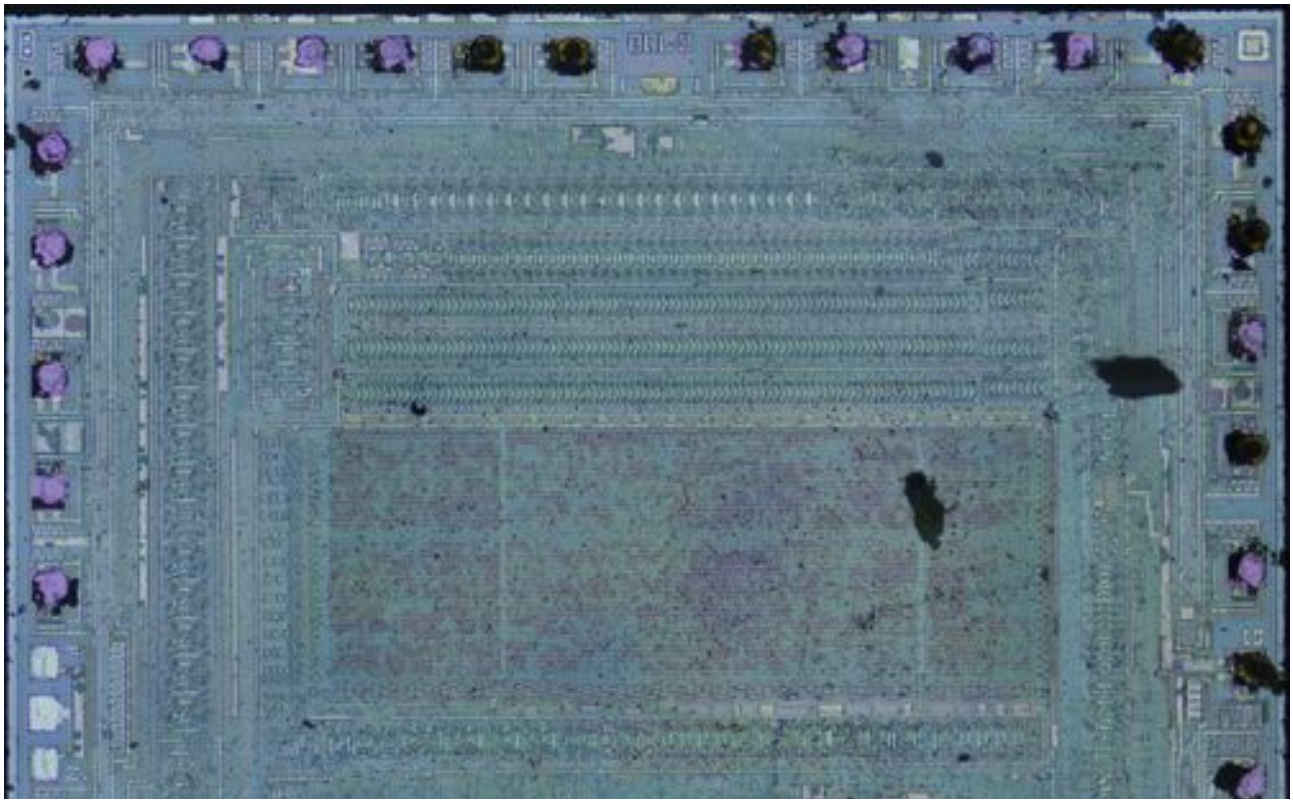


Illustration 1: Disk drive IC





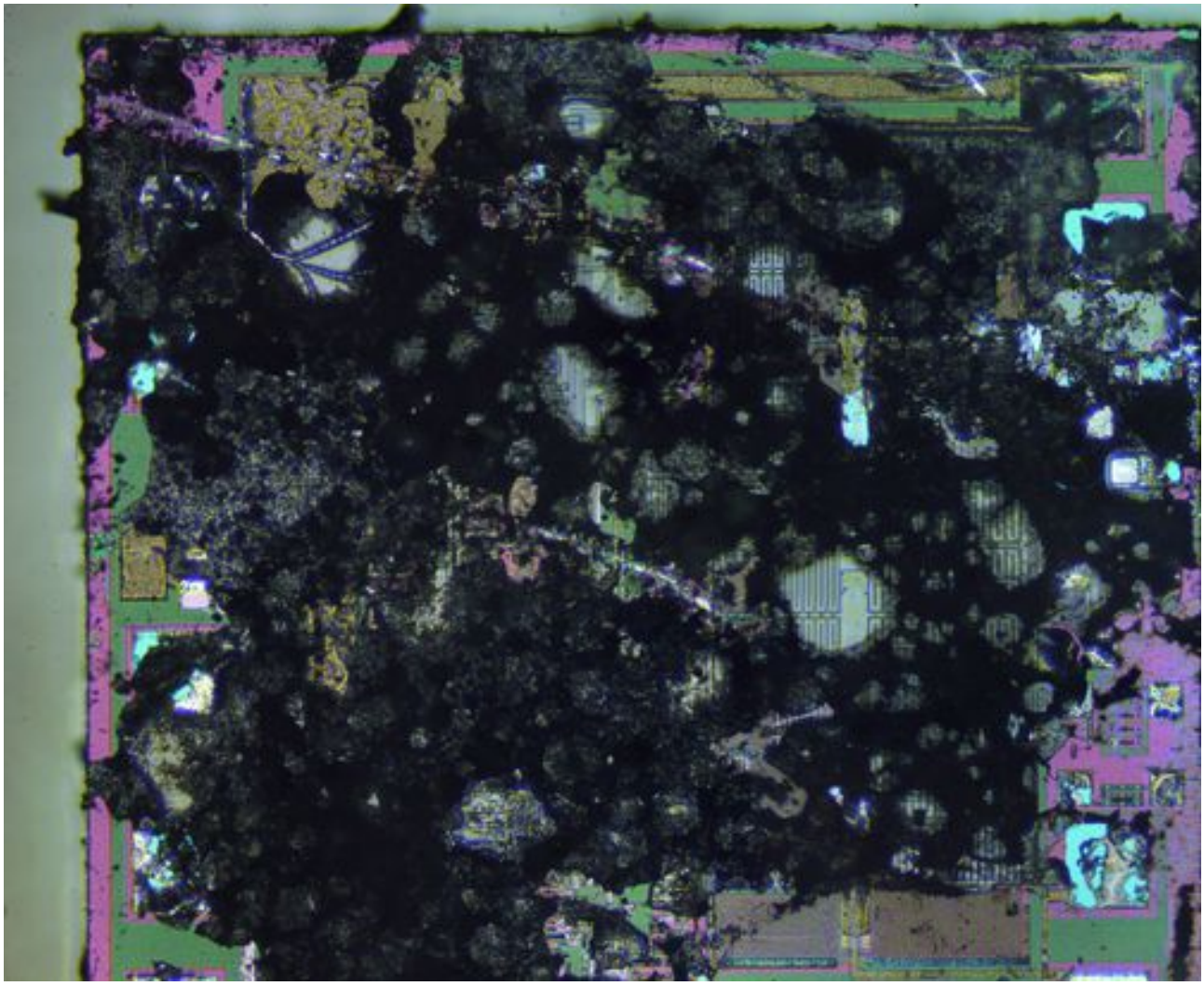


Illustration 4: Quartz watch IC with no cleaning

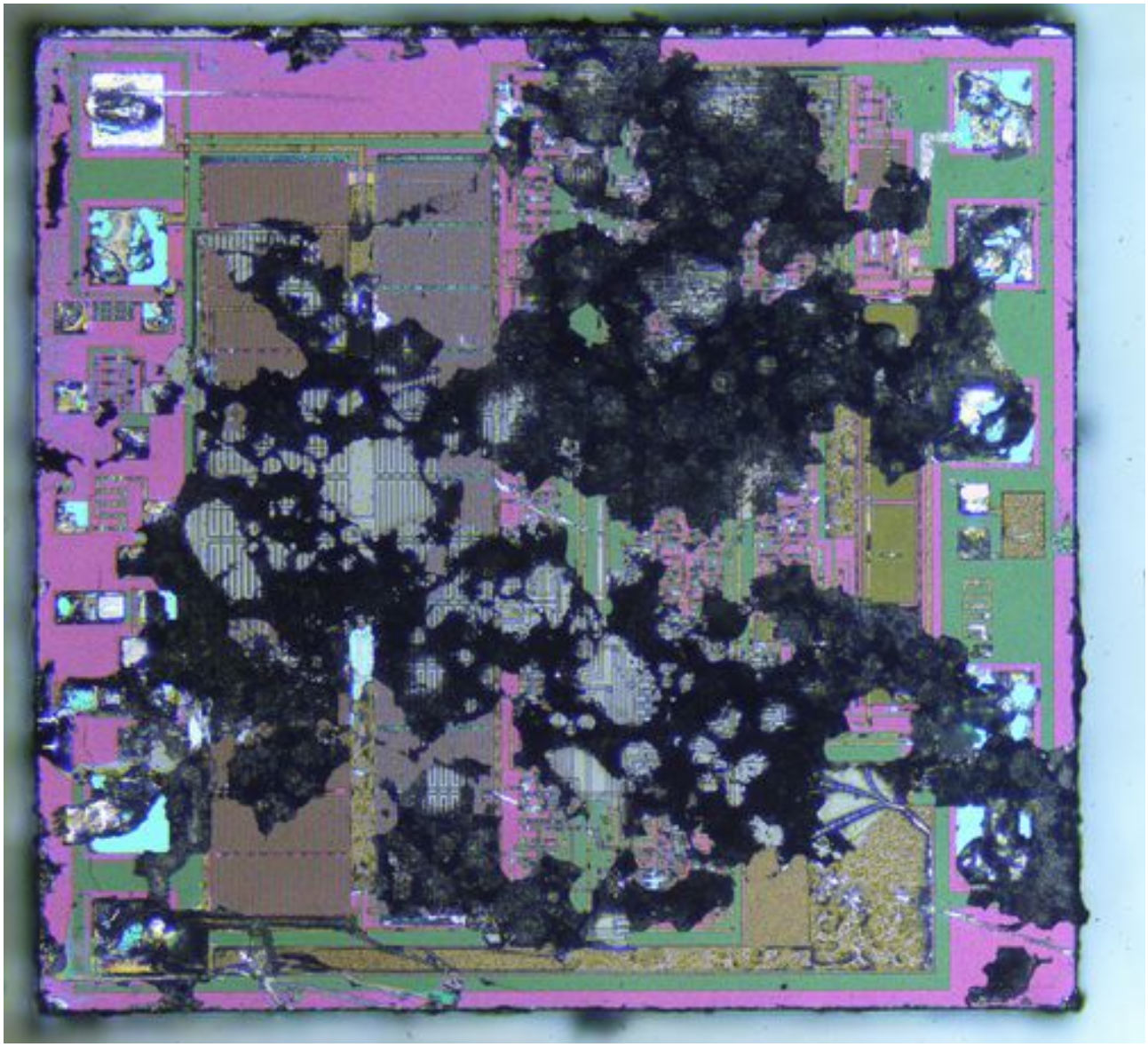


Illustration 5: Quartz watch IC after 3 minutes of ultrasonic cleaning

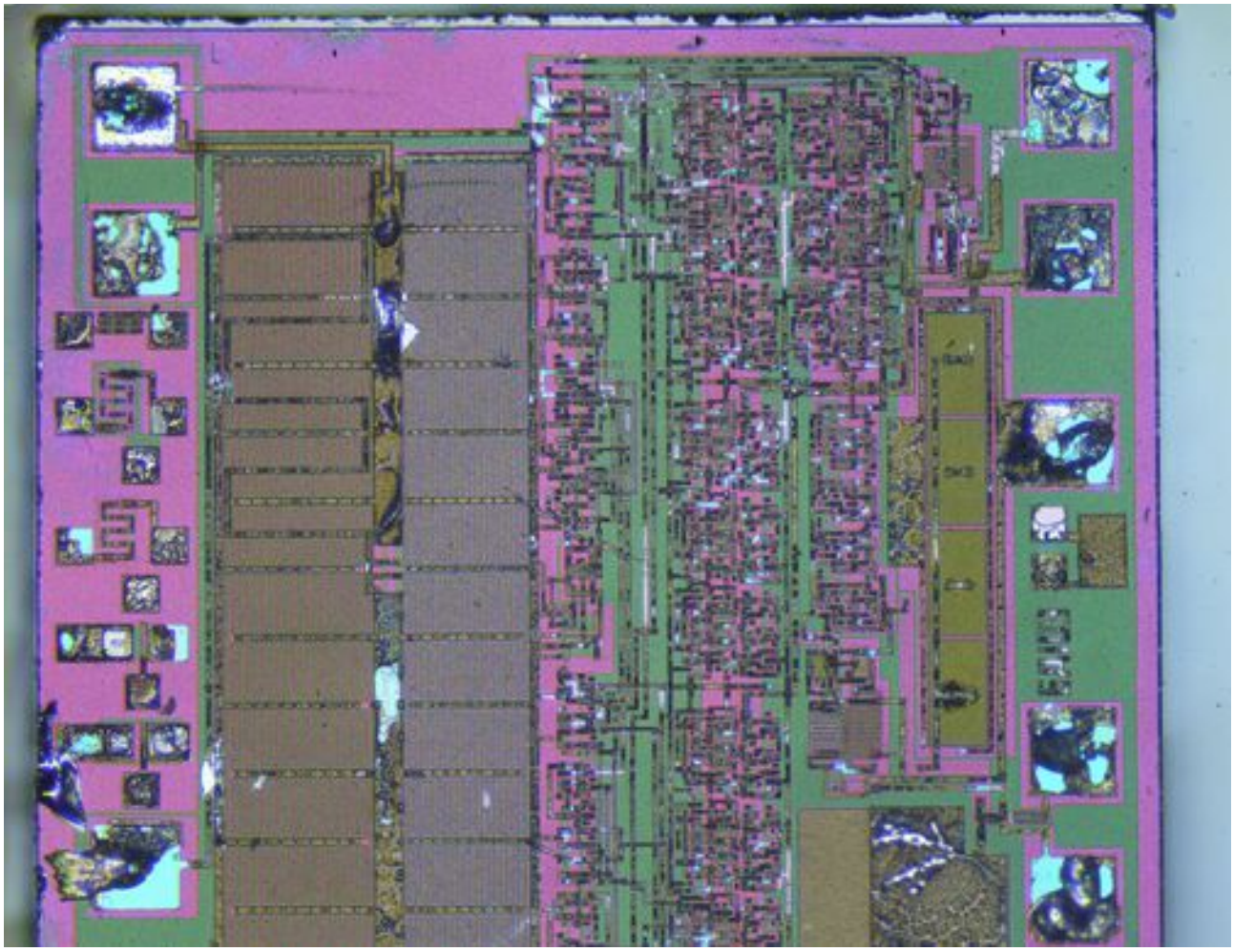


Illustration 6: Quartz watch IC after a second heating and a further 3 minutes of ultrasonic cleaning

I have a video of the decapping of a quartz watch IC on my Youtube channel. Link:

https://youtu.be/jxPNGlKMGYM

Comments to the author are welcomed, email: menadue AT gmail DOT com

Published in the April 2018 issue of *Micscape* magazine.

www.micscape.org