How to Destroy a Laptop with Top Secrets

How GCHQ supervised The Guardian's destruction of machines storing Snowden's documents

@musalbas and @richietynan
Privacy International

Background

- The Guardian had copies of Snowden documents in their London office.
  - Stored on encrypted and airgapped machines in a secure room.
  - Round-the-clock guards and a ban on electronics.
- The Guardian was reporting on these documents.
- The British government wasn't happy about this.

Threats

- Cabinet secretary (Jeremy Heywood) pressured The Guardian to return the documents.
  - To conduct “forensics”. (Oliver Robbins, national security advisor)
  - To strengthen the legal case against Snowden and The Guardian.
- The ~~threats~~ harassment continued.
  - Heywood: "We can do this nicely or we can go to law", "A lot of people in government think you should be closed down."
  - Robbins: “If you won't return it [the Snowden material] we will have to talk to 'other people' this evening.”

Responding to threats

- The Guardian had to protect itself, but continue to report on the documents, by destroying its London copy of the documents.
- GCHQ wanted to inspect the material before destruction, destroy it themselves and then take the destroyed pieces.
  - The Guardian disagreed.
- Mutual agreement: The Guardian would destroy it themselves, under the supervision of GCHQ.

Destruction

- GCHQ instructed the Guardian to buy angle-grinders, dremels (drills with revolving bits), and masks.
  - GCHQ provided a degausser (destroys magnetic fields and erases data), as it was expensive.
- GCHQ supervised the instruction process.
- 2 GCHQ technical experts recorded the process with their iPhones.

Destruction video

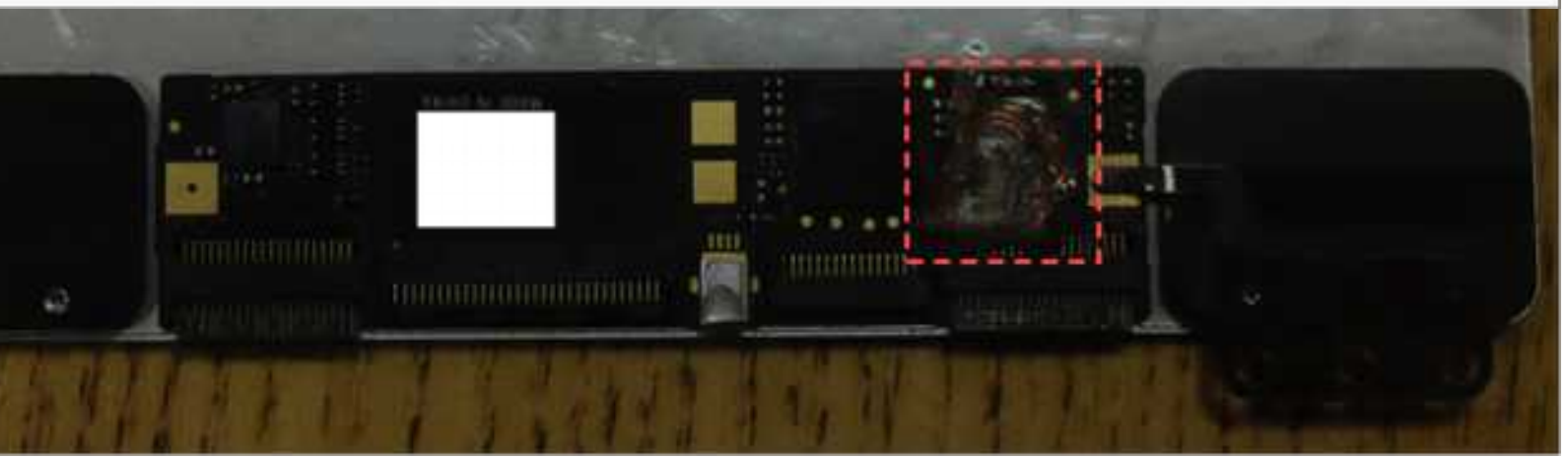
- http://www.theguardian.com/uk-news/2014/jan/31/footage-released-guardian-editors-snowden-hard-drives-gchq

Aftermath

- Why did GCHQ supervise the Guardian to destroy in a specific way?
- There could be a lot to learn from GCHQ about how to properly eradicate data from a device.
- Many non-obvious components were destroyed, including components in the keyboard, trackpad, battery controller...

Trackpad controller

Before



After:
Destroyed serial flash chip.
Macronix MX25L2006E stores up to 2M-BIT.

Mac firmware updates

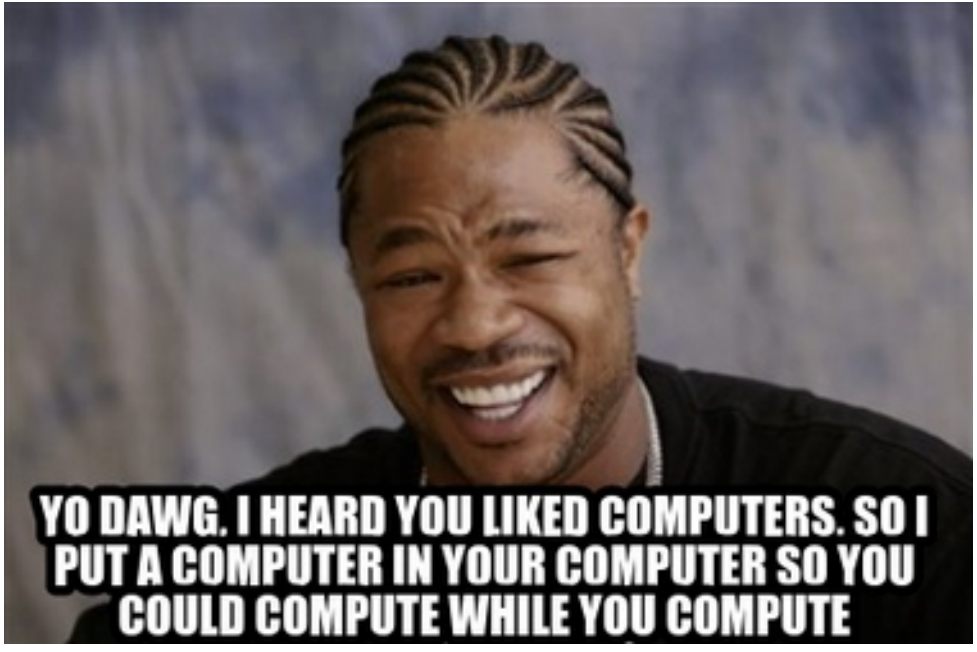
MacBook Pro (Retina) Trackpad Update 1.0

Download

Mac firmware updates

Xzibit's Iron Law of Computer Architecture

- Via Dan Kaminsky 2014 Defcon talk.
- Hard work is offloaded to hardware, which is really just another computer - with its own firmware and storage.
- The biggest lie about your computer is that it's just one computer.



Is GCHQ trolling?

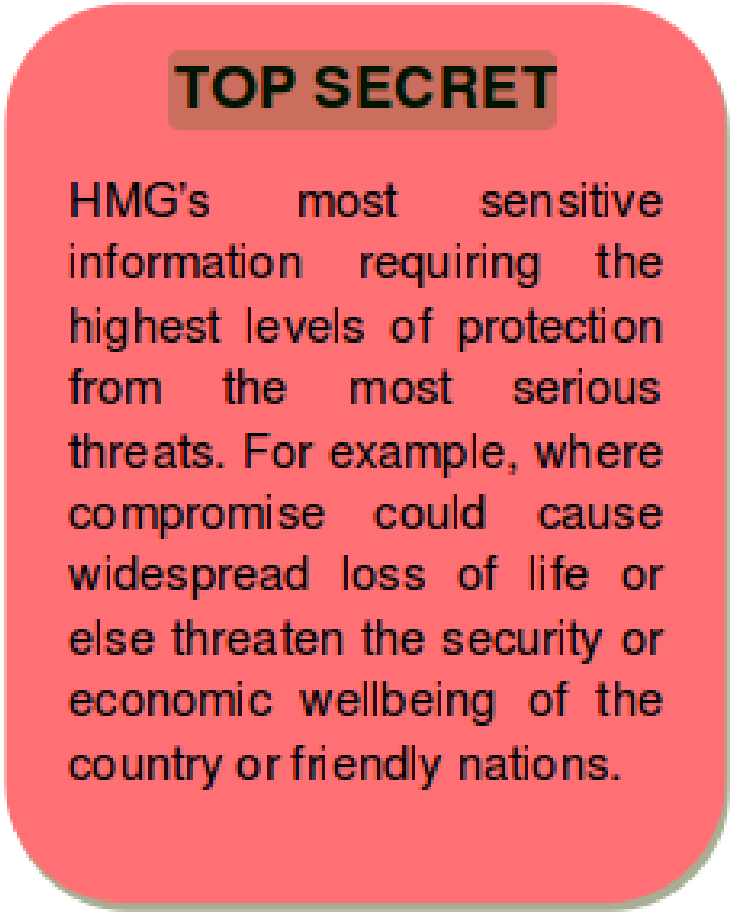
- Joint Threat Research Intelligence Group (JTRIG)
  - “The scope of the JTRIG's mission includes using "dirty tricks" to “destroy, deny, degrade [and] disrupt” enemies by “discrediting” them, planting misinformation and shutting down their communications.”
- "It was purely a symbolic act," Johnson said. "We knew that. GCHQ knew that. And the government knew that." - Guardian staff member Paul Johnson
- Was it a purely symbolic act from a technical standpoint?
- GCHQ didn't intended for the destruction or the devices to be public; they originally just wanted the machines intact to conduct forensics.
- Is GCHQ spreading disinformation?
  - Maybe - probably not, but evidence suggests that destroying these chips is actually a good idea.

Claims

- Claims by commentators after our original article about the destroyed hardware:
- “Back when I worked for Convergys/Apple, one of the main things was we could not bring in our own peripherals to use. Mice, keyboard, etc. The issue is that one, in theory, could customize it for storage covertly and copy customer/client information.”
- “I have destroyed the brand new iDevices of senior Government personnel because they plugged it into a classified network to charge it for less than a minute. The law is the law. I actually had a wall of digital devices we had drilled, degaussed etc.”

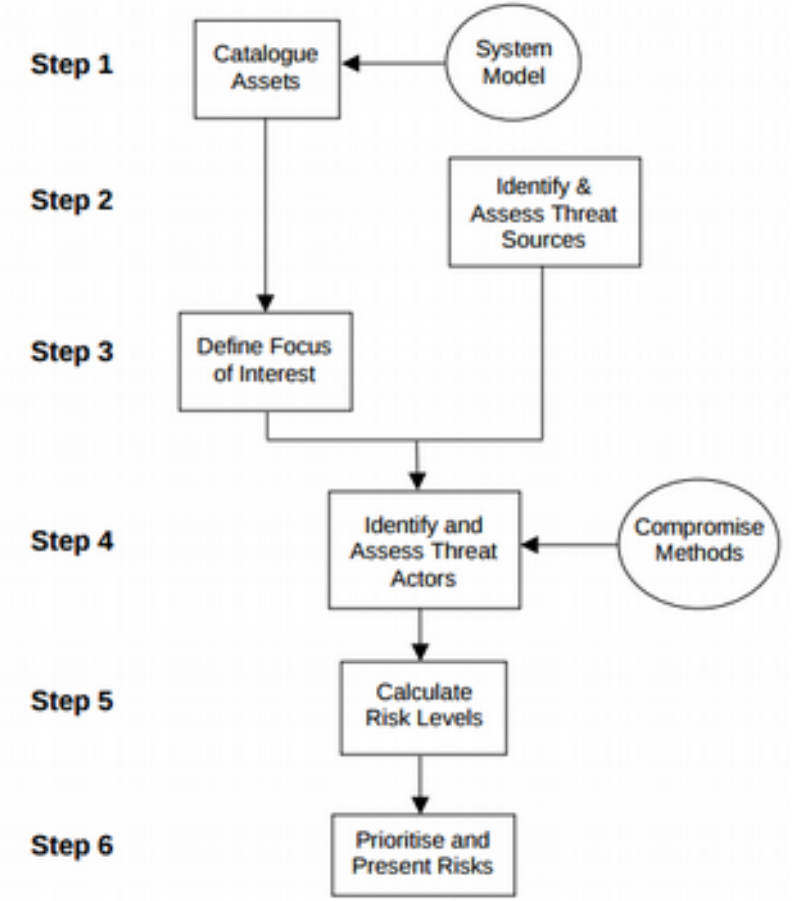
“Top secret”

- What *is* the law?
- A document from the Cabinet Office (“Government Security Classifications”) defines “Top secret” and its threat model in great detail.



HMG IA Standard No. 1

- By Communications-Electronics Security Group, a group within GCHQ.
- A document for assessing technical risks to government information.



“Top secret” threat profile

- From “Government Security Classifications”.

The threat profile for **TOP SECRET** reflects the highest level of capability deployed against the nation’s most sensitive information and services. It is assumed that advanced state actors will prioritise compromising this category of information or service, using significant technical, financial and human resources over extended periods of time. Highly bespoke and targeted attacks may be deployed, blending human sources and actions with technical attack. Very little information risk can be tolerated.

Implants from the NSA ANT catalog

TOP SECRET//COMINT//REL TO USA, FVEY

SURLYSPAWN

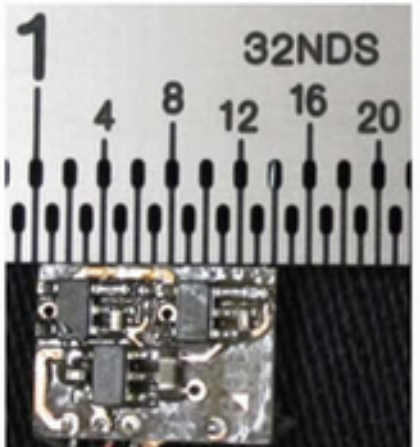
ANT Product Data

(TS//SI//REL TO USA,FVEY) Data RF retro-reflector. Provides return modulated with target data (keyboard, low data rate digital device) when illuminated with radar.

07 Apr 2009

(U) Capabilities

(TS//SI//REL TO USA,FVEY) SURLYSPAWN has the capability to gather keystrokes without requiring any software running on the targeted system. It also only requires that the targeted system be touched once. The retro-reflector is compatible with both USB and PS/2 keyboards. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities will include laptop keyboards.



GCHQ procedures

- Documents that govern counter-compromise measures:
  - HMG Information Assurance Note 5
    - Data destruction standard used by the British government.
    - I emailed GCHQ to ask nicely for a copy... they refused. :(
    - “CESG's policy and guidance is only available to UK Public Sector organisations. Therefore we are not able to issue a copy of the document to you.”
    - “Communications with GCHQ may be monitored and/or recorded for system efficiency and other lawful purposes.”
  - Joint Services Publication 440
    - Ministry of Defence 2,400-page restricted security manual.
    - Leaked by WikiLeaks.

Joint Services Publication 440

- “ERASURE OF PROTECTIVELY MARKED COMPUTER STORAGE MEDIA”
- Footnote for 7: “Destroy – Disintegrate, incinerate, pulverise, shred or melt.”

SEMI-CONDUCTOR MEMORY	RE-USE		DISPOSAL		REPAIR/EXCHANGE	
	Baseline Standard	*Enhanced Standard*	*Baseline Standard*	*Enhanced Standard*	*Baseline Standard*	*Enhanced Standard*
RAM	Overwrite[1]	Overwrite[2]	Overwrite[1] then remove all power, or destroy[7]	Overwrite[2] then remove all power, or destroy[7]	Overwrite[1] then remove all power	Overwrite[2], then remove all power
DRAM	Overwrite[1] or remove all power	Overwrite[2] then remove all power	Overwrite[1] then remove all power, or destroy[7]	Overwrite[2], or destroy[7]	Overwrite[2], then leave powered-up for 72 hours	Overwrite[2,3], then leave powered-up for 72 hours
EPROM	UV erase[4]	UV erase[5]	UV erase[4], then Overwrite[1], or destroy[7]	UV erase[5] then Overwrite[2] or destroy[7]	UV erase[4], then Overwrite[1]	UV erase[5] then Overwrite[2]
FLASH EPROM	Chip erase[6] or Overwrite[1]	Chip erase[6] then Overwrite[2]	Chip erase[6] then Overwrite[1], or destroy[7]	Chip erase[6] then Overwrite[2], or destroy[7]	Chip erase[6] then Overwrite[1]	Chip erase[6] then Overwrite[2]
EEPROM	Chip erase[6] or Overwrite[1]	Chip erase[6] then Overwrite[2]	Chip erase[6] or Overwrite[1] or destroy[7]	Chip erase[6] then Overwrite[2] or destroy[7]	Chip erase[6] then Overwrite[2,3]	Chip erase[6] then Overwrite[2,3]
OTHER DEVICES	Destroy[7]	Destroy[7] or seek CESG advice	Destroy[7] or seek CESG advice	Destroy[7] or seek CESG advice	Destroy[7] or seek CESG advice	Destroy[7] or seek CESG advice

Joint Services Publication 440

- "The security measures in this chapter are aimed primarily to cover contacts made in CSSRAs and have been drawn up to protect the individual from action by FISs, extremist groups, investigative journalists and criminals."

Top Secret Sanitisation – New Zealand

Hybrid hard drives, Solid State Drives and Flash Memory Devices

13.4.6. Hybrid hard drives, solid state drives and flash memory devices are difficult or impossible to sanitise effectively. In most cases safe disposal will require destruction. The

Pre-sanitisation classification / Caveat	Post-sanitisation classification / Caveat
New Zealand Eyes Only (NZEO) Caveat	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED and all lower classifications	UNCLASSIFIED

Volatile Storage e.g. RAM

Pre-sanitisation classification	Post-sanitisation classification
New Zealand Eyes Only (NZEO) Caveat	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED	UNCLASSIFIED

Non-volatile Storage e.g. HDD

Same for SSDs and Hybrid drives, Flash, EPROM and EEPROM

Top Secret Destruction – New Zealand

Item	Destruction methods					
	Furnace/ Incinerator	Hammer mill	Disintegrator	Grinder/ Sander	Cutting	Degausser
Magnetic floppy disks	Yes	Yes	Yes	No	Yes	Yes
Magnetic hard disks	Yes	Yes	Yes	Yes	No	Yes
Magnetic tapes	Yes	Yes	Yes	No	Yes	Yes
Optical disks	Yes	Yes	Yes	Yes	Yes	No
Electrostatic memory devices	Yes	Yes	Yes	Yes	No	No
Semi-conductor memory	Yes	Yes	Yes	No	No	No

Top Secret Destruction – New Zealand

Initial media classification	Screen aperture size particles can pass through			
	Less than or equal to 3mm	Less than or equal to 6mm	Less than or equal to 9mm	Less than or to 12mm
TOP SECRET	UNCLASSIFIED	RESTRICTED	CONFIDENTIAL	SECRET
SECRET	UNCLASSIFIED	UNCLASSIFIED	RESTRICTED	CONFIDENTIAL
CONFIDENTIAL	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	RESTRICTED
RESTRICTED	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED

Top Secret Destruction – New Zealand

13.5.11.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST perform the destruction of accountable material under the supervision of at least two personnel cleared to the highest classification of the media being destroyed.

Top Secret Destruction – Australia

Circumstances preventing reclassification of volatile media

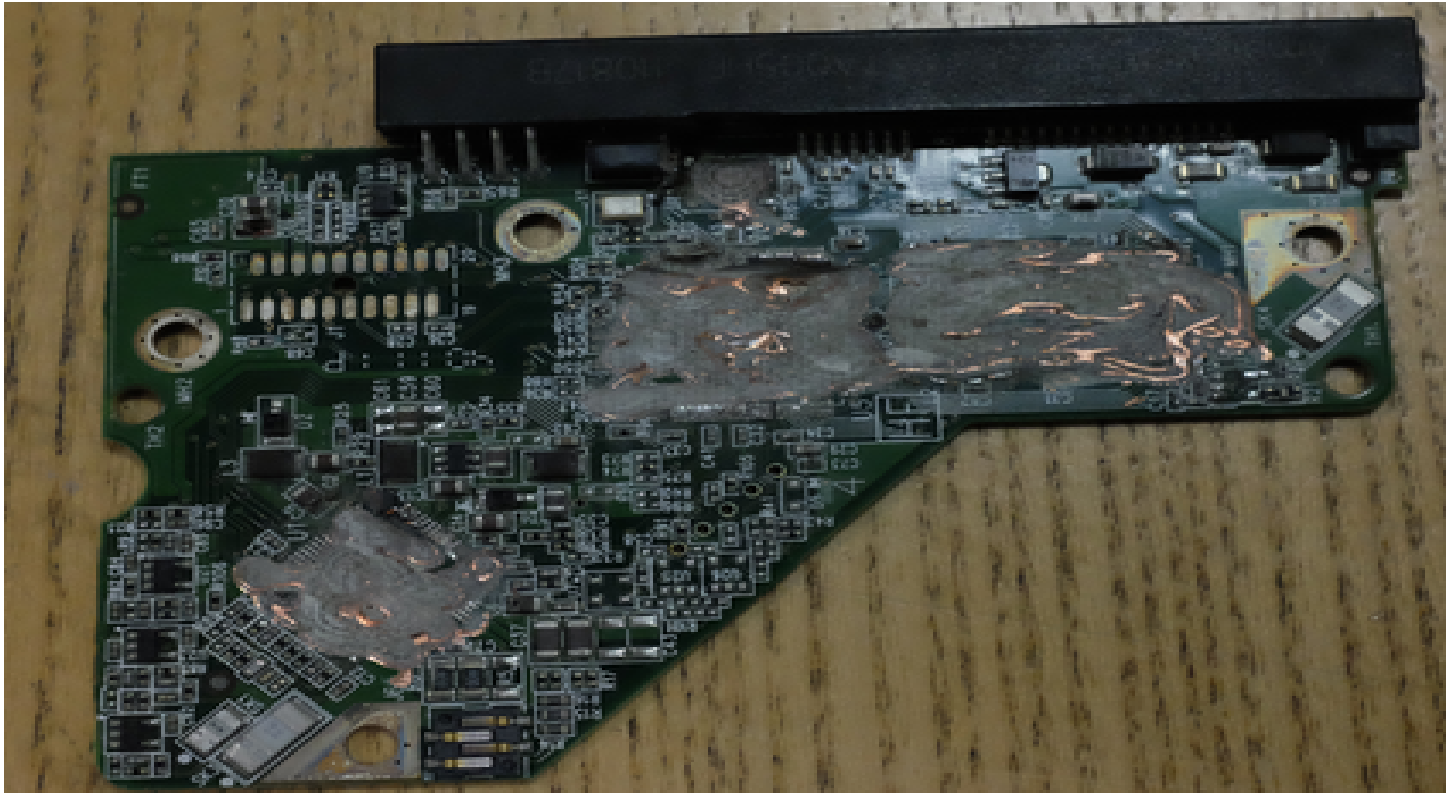
Typical circumstances preventing the reclassification of TOP SECRET volatile media include a static cryptographic key being stored in the same memory location during every boot of a device and a static image being displayed on a device and stored in volatile media for a period of months.

Treatment of non–volatile magnetic media following sanitisation

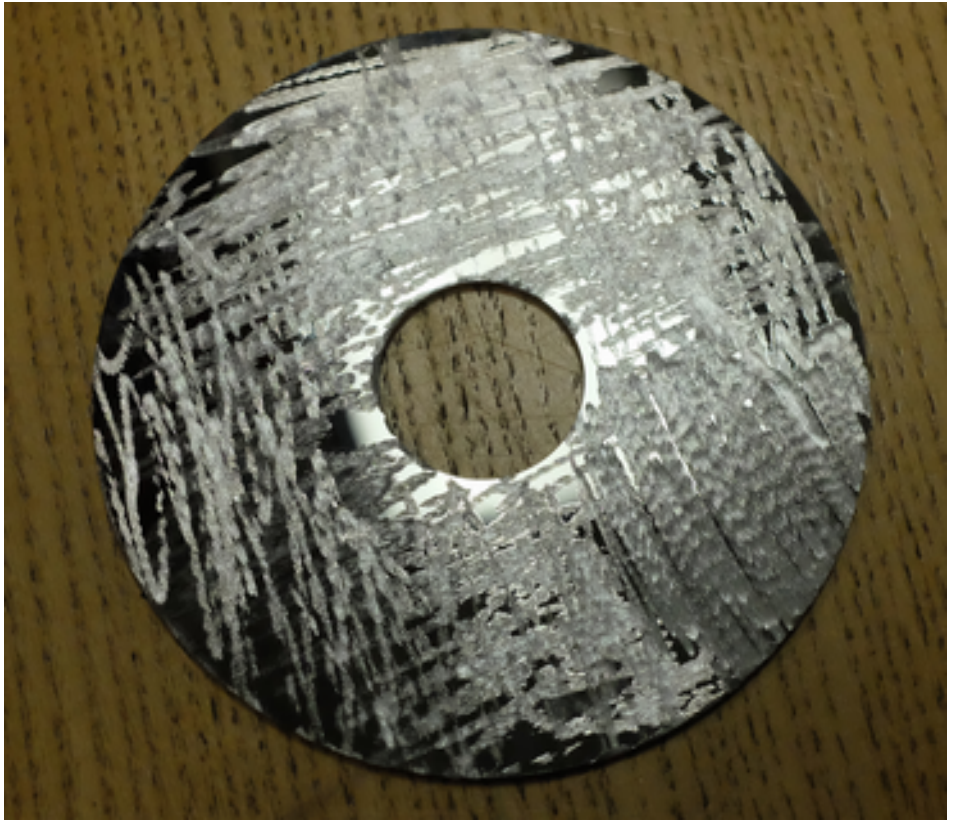
Highly classified non–volatile magnetic media cannot be sanitised below its original classification due to concerns with the sanitisation of the host protected area, device configuration overlay table and growth defects table. The sanitisation of TOP SECRET non–volatile media does not allow for the reduction of its classification.

RAM

Hard drive controller



Hard drive platter



Top Secret Destruction – Australia

Treatment of non–volatile flash memory media following sanitisation

Due to the use of wear levelling in flash memory, it is possible that not all physical memory locations are written to when attempting to overwrite the media. Information can therefore remain on the media. This is why TOP SECRET, SECRET and CONFIDENTIAL flash memory media must always remain at their respective classification, even after sanitisation.

ITEM	DESTRUCTION METHODS					
	FURNACE/ INCINERATOR	HAMMER MILL	DISINTEGRATOR	GRINDER/ SANDER	CUTTING	DEGAUSSER
Electrostatic memory devices	Yes	Yes	Yes	Yes	No	No
Magnetic floppy disks	Yes	Yes	Yes	No	Yes	Yes
Magnetic hard disks	Yes	Yes	Yes	Yes	No	Yes
Magnetic tapes	Yes	Yes	Yes	No	Yes	Yes
Optical disks	Yes	Yes	Yes	Yes	Yes	No
Semiconductor memory	Yes	Yes	Yes	No	No	No

INITIAL MEDIA HANDLING	SCREEN APERTURE SIZE PARTICLES CAN PASS THROUGH			
	LESS THAN OR EQUAL TO 3MM	LESS THAN OR EQUAL TO 6MM	LESS THAN OR EQUAL TO 9MM	LESS THAN OR EQUAL TO 12MM
TOP SECRET	Unclassified	PROTECTED	CONFIDENTIAL	SECRET
SECRET	Unclassified	Unclassified	PROTECTED	CONFIDENTIAL
CONFIDENTIAL	Unclassified	Unclassified	Unclassified	PROTECTED
PROTECTED	Unclassified	Unclassified	Unclassified	Unclassified
Unclassified (DLM)	Unclassified	Unclassified	Unclassified	Unclassified

Top Secret Destruction – Canada & USA

PC, C, S, TS	Miniature drives or Flash/EEPROM devices: • grind or pulverize the storage chip or the entire storage device into small pieces < 2mm in size, using a 3/32-inch screen.

c) Disintegration: Disintegrate into particles that are nominally 2 millimeter edge length in size. It is highly recommended to disintegrate hard disk drive storage devices in bulk lots with other storage devices.

Top Secret Destruction – UK

IA5 FEATURES THREE TIERS FOR PHYSICAL DESTRUCTION:

Secure Sanitisation Level 1 (SSL1), is for information that is Protectively Marked "Unclassified – IL1" and "Protect – IL2". IA5 states that IL1 & 2 information be destroyed to Commercial Best Practice standards. Data Eliminate's truck mounted shredder/disintegrator shreds computer hard disks and magnetic tapes to this Commercial Best Practice specification.

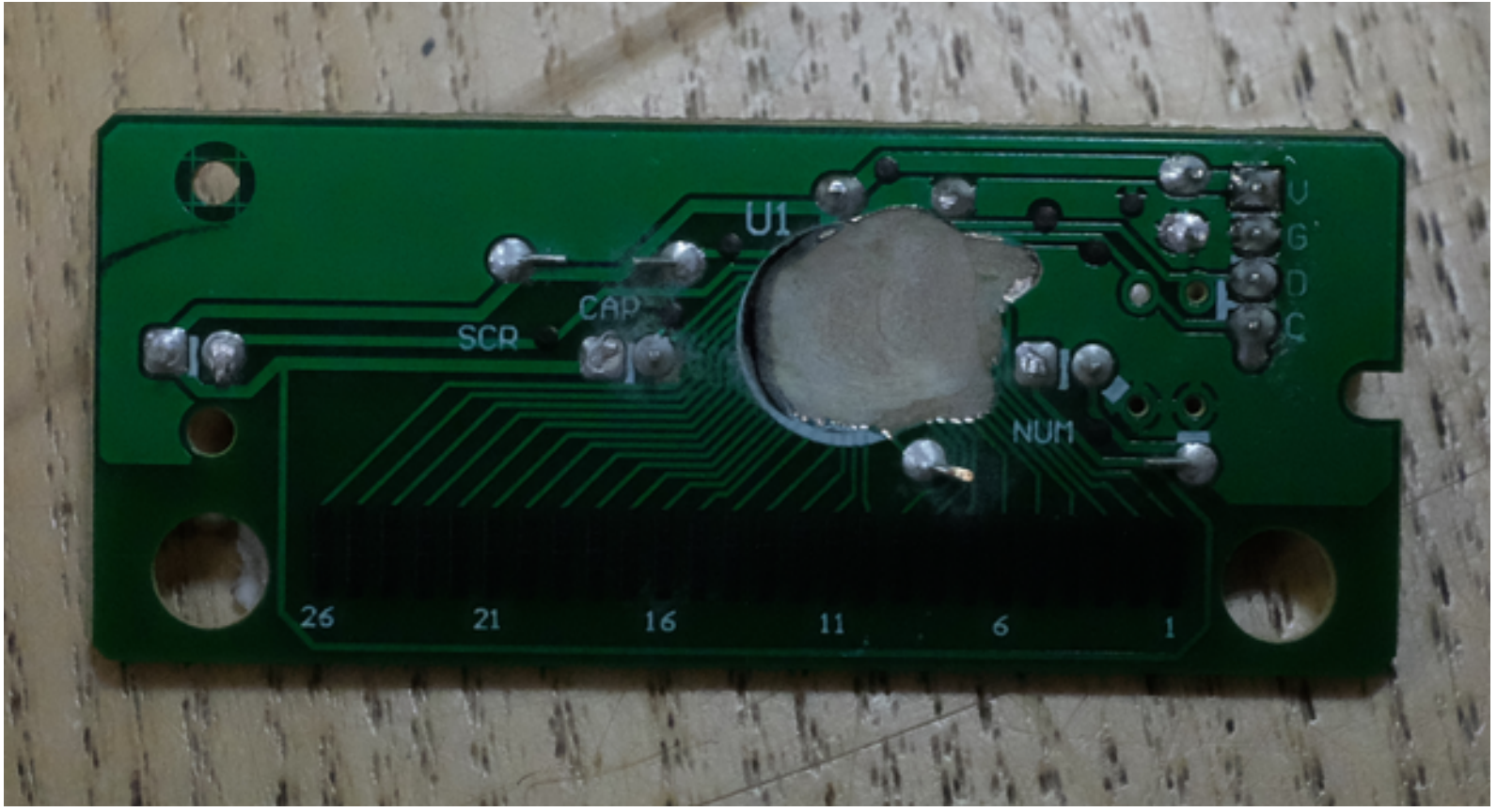
Secure Sanitisation Level 2, SSL2, is for information that is Protectively Marked "Restricted – IL3" and "Confidential – IL4". IA5 states that IL3 information needs to be degaussed or shredded in line with the Lower Level Degaussing Standard. Eg That when the data bearing device is reconnected to a reading device cannot be read. For IL4 Confidential both degaussing and shredding are required for off-site services. This work should normally be done by SC cleared staff.

Crown Commercial Service

Secure Sanitisation Level 3, SSL3, is for information that is Protectively Marked "Secret – IL5" and "Top Secret – IL6". IL5 & 6 media must be degaussed to CESG's Higher Level and shredded to 6mm particles if the media is magnetic media, and shredded to 2mm particles if the media is optical.

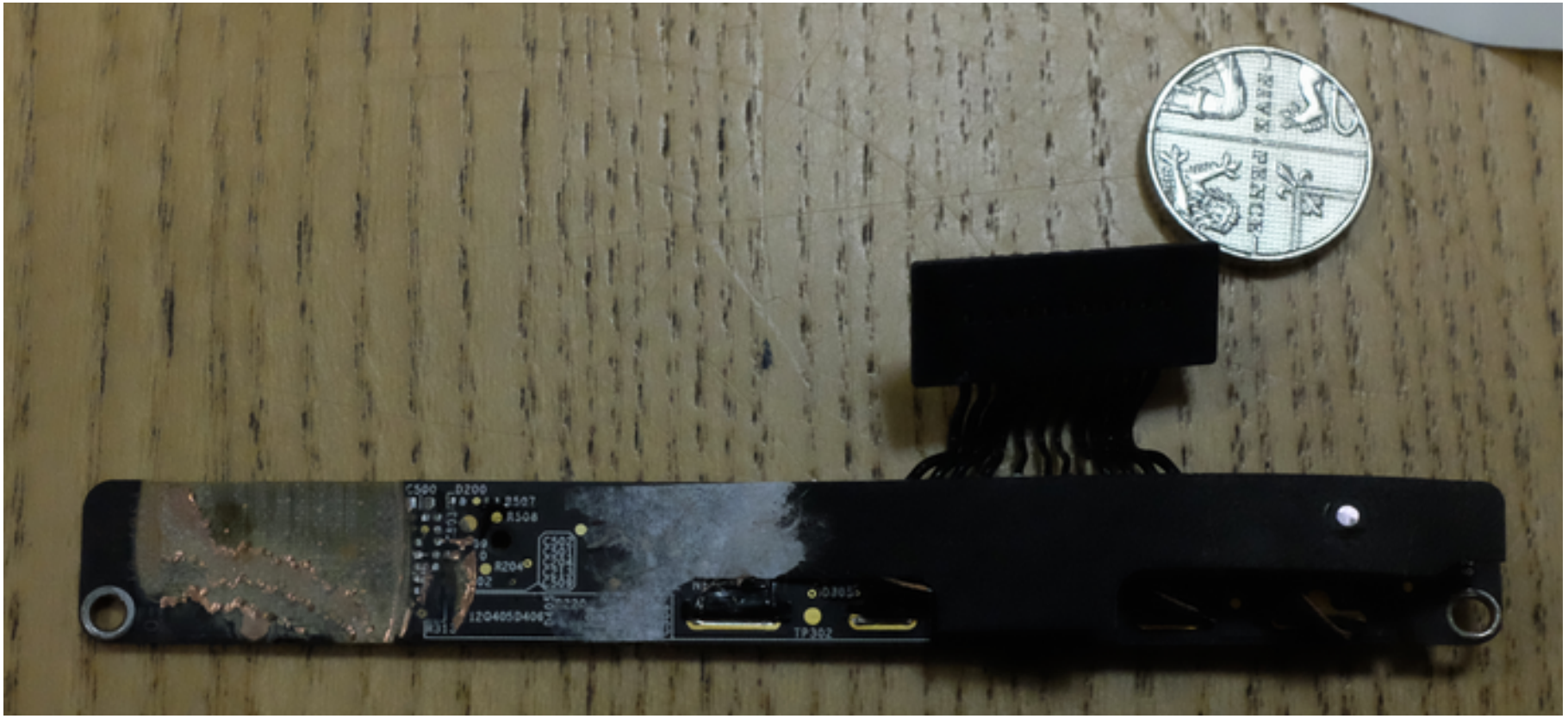
http://www.secure-data-destruction.co.uk/impact-level/

Keyboard Controller

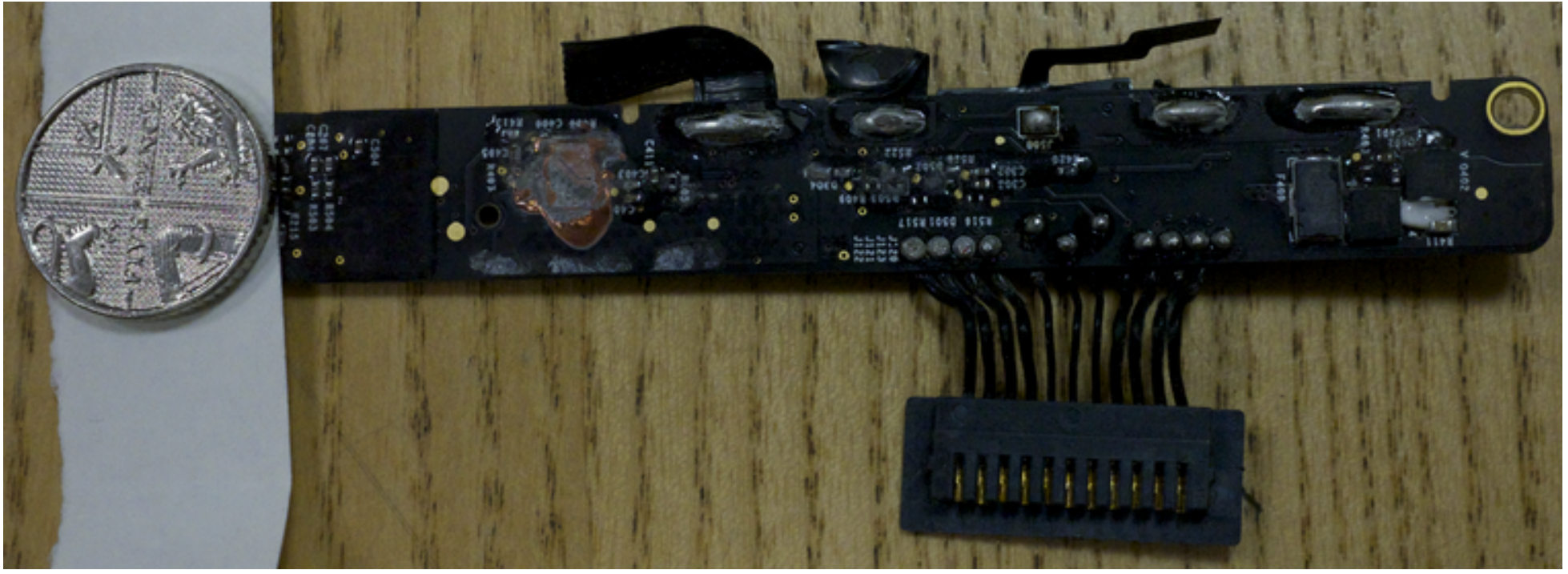


Keyboard and Trackpad Controller

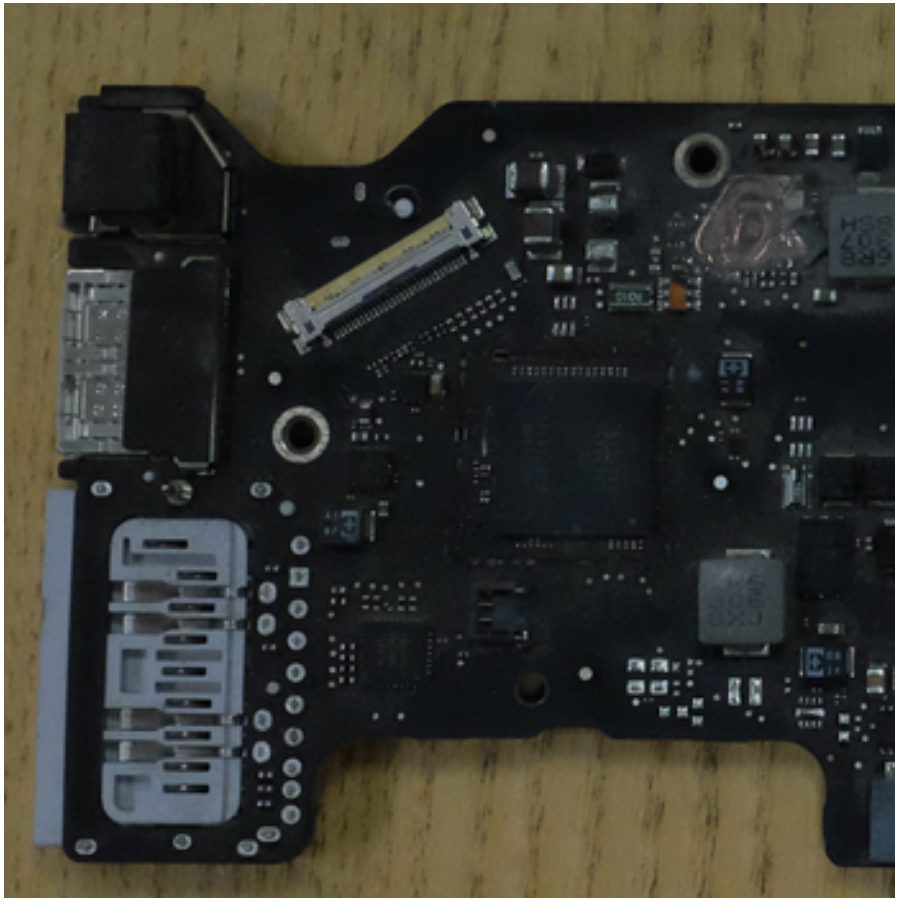
Power Controller



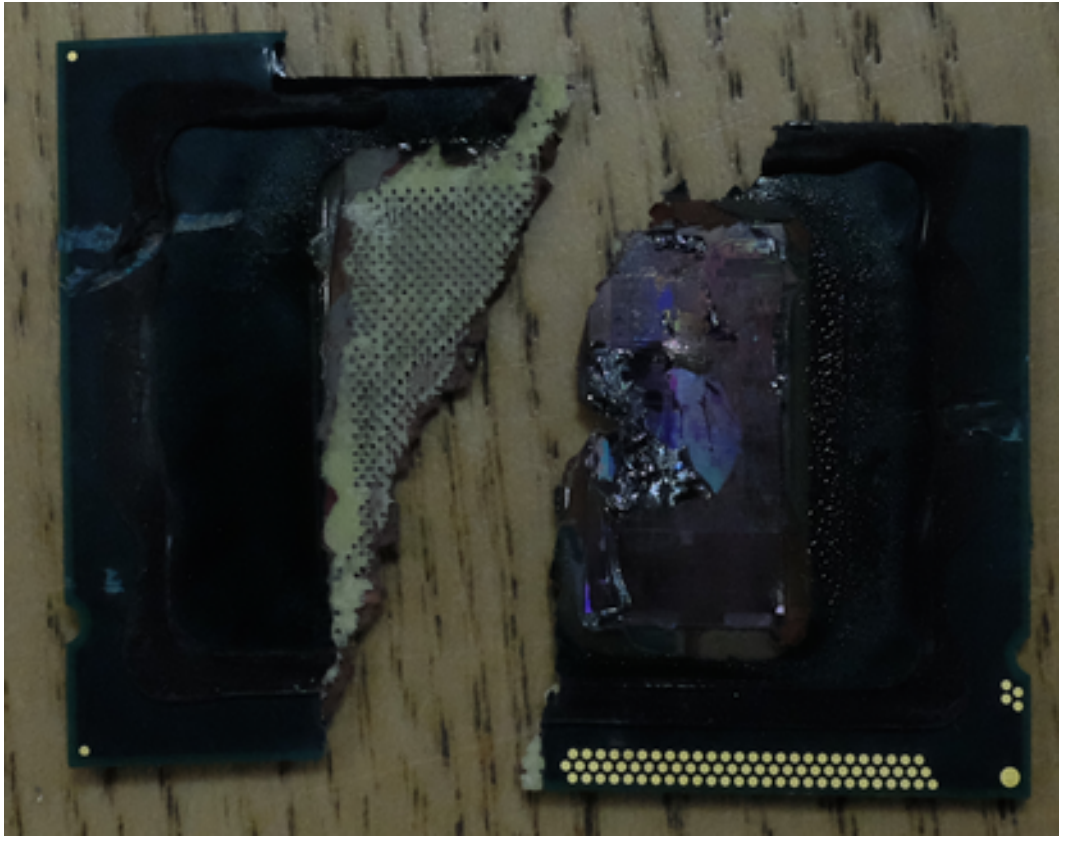
Power Controller



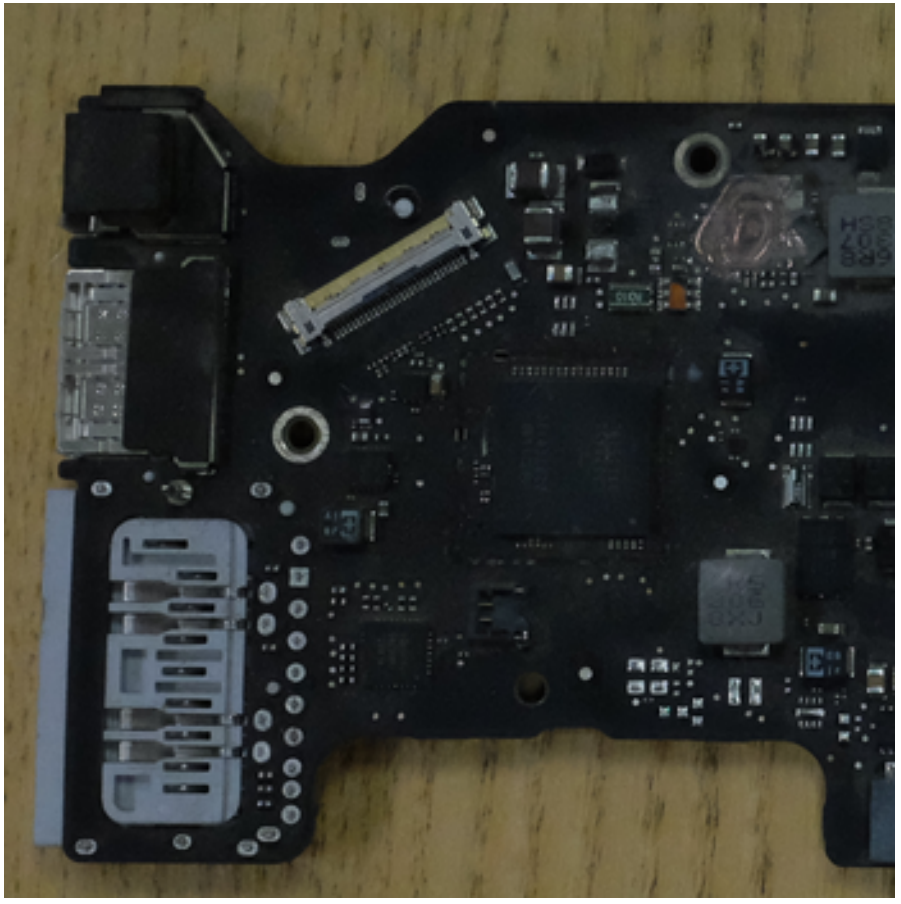
Inverting Converter



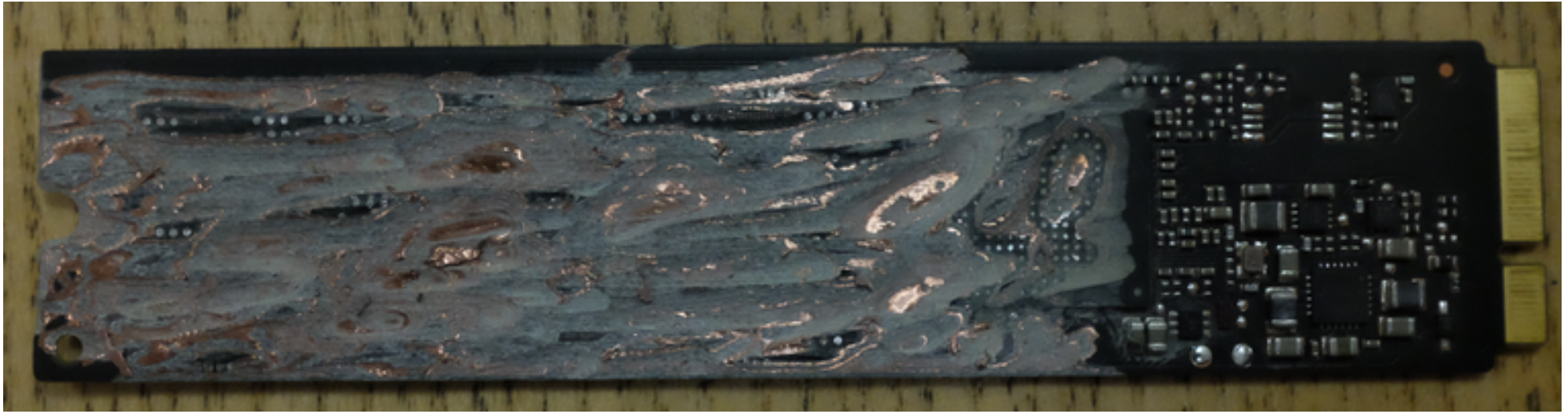
CPU



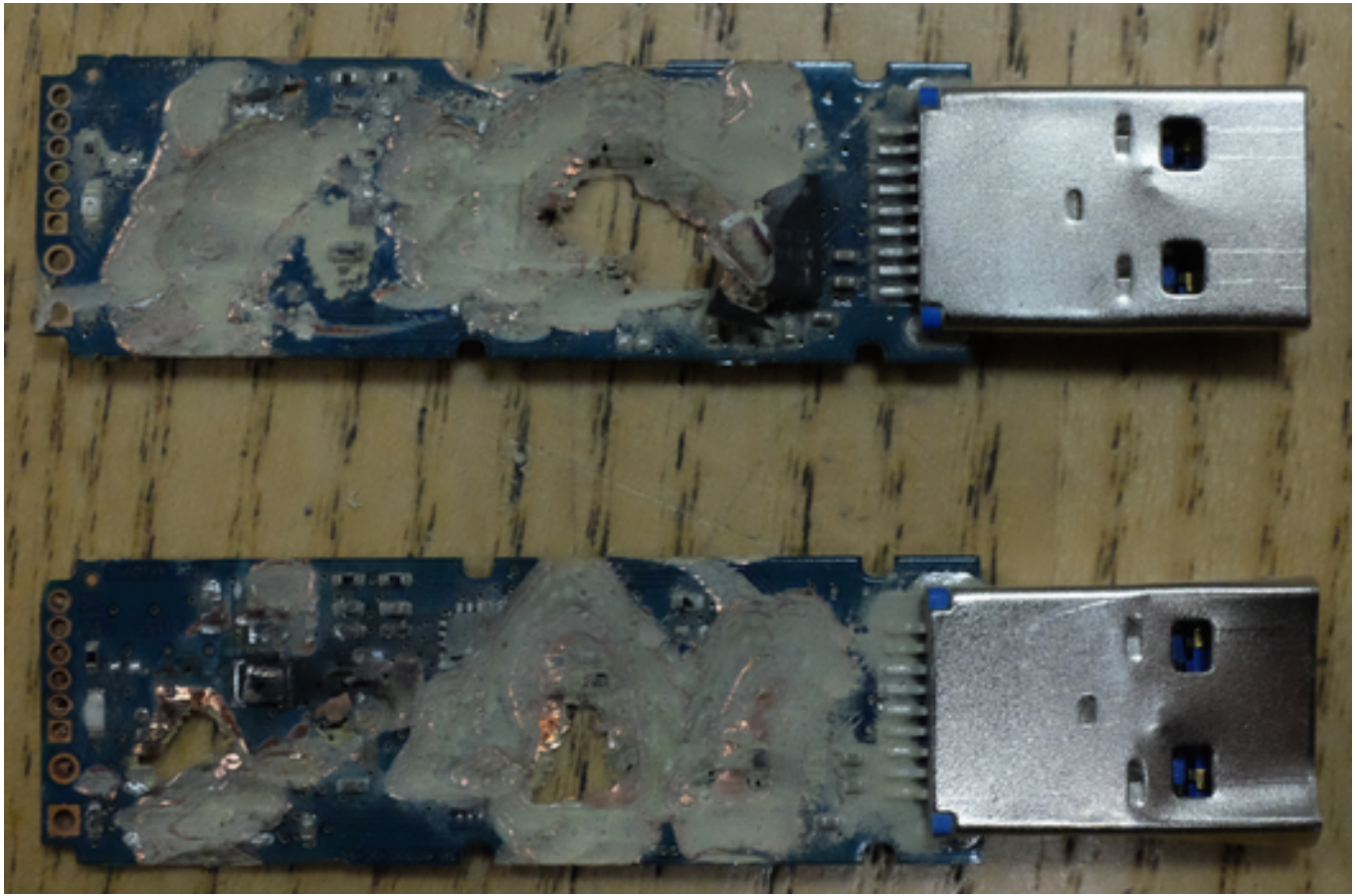
Inverting Converter



SSD



USB Sticks



USB Sticks

USB Sticks

Recap

- GCHQ doesn't trust Apple devices to keep its secrets – should we?
- If a component contains Top Secret material it must be destroyed as per the guidelines
- Which components contain Top Secret material?
- Now we know this for the specific Mac Book Air model in question
- What about all other computers?

ht @csoghoian

Companies Responses: Dell

- Dell sources parts from multiple vendors and our program engineering team confirms the usage of the product and ensures the right electronic design is used for end users purpose as per the global standards.
- We regret to inform you that we would not be able to share any circuitry design modules /sourcing details as its Dell confidential.
- the USB keyboards provided by Dell are used only as Input device and does not have the capability to store any data or layout data.

Companies Responses: HP

- Proceeding to get the information from HP
-
-
-
- **Confidential**
-
- Hi Gus and Richard,
-
-
- Accordingly, we would like to make all interactions between PI and the companies public. Could you please confirm that it is ok for us to do so in relation to HP. We think that this process needs to be as transparent as the end result.

Theories

- All just a show of power and no information can be gleaned from the chips destroyed.
- “Back when I worked for Convergys/Apple, one of the main things was we could not bring in our own peripherals to use. Mice, keyboard, etc. The issue is that one, in theory, could customize it for storage covertly and copy customer/client information.”
- “I have destroyed the brand new iDevices of senior Government personnel because they plugged it into a classified network to charge it for less than a minute. The law is the law. I actually had a wall of digital devices we had drilled, degaussed etc.”
- Obvious to some people what they did.

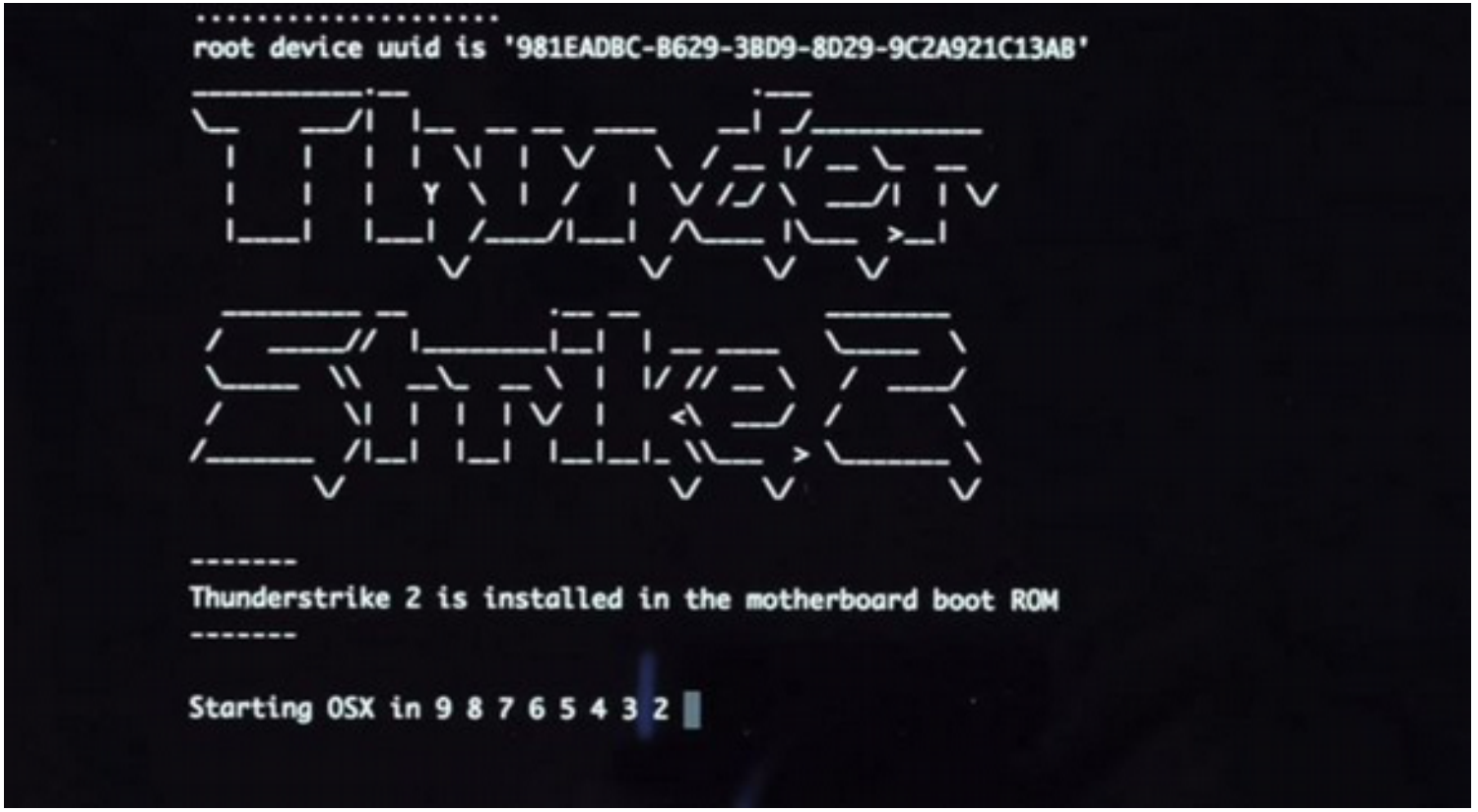
Theories

- GCHQ were destroying traces of malware they had installed
- GCHQ were removing places where their malware could store data
- GCHQ were removing places where malware could store data
- Some components could store data but others couldn't – misinformation.
- Any more from the audience?

Why is this important?

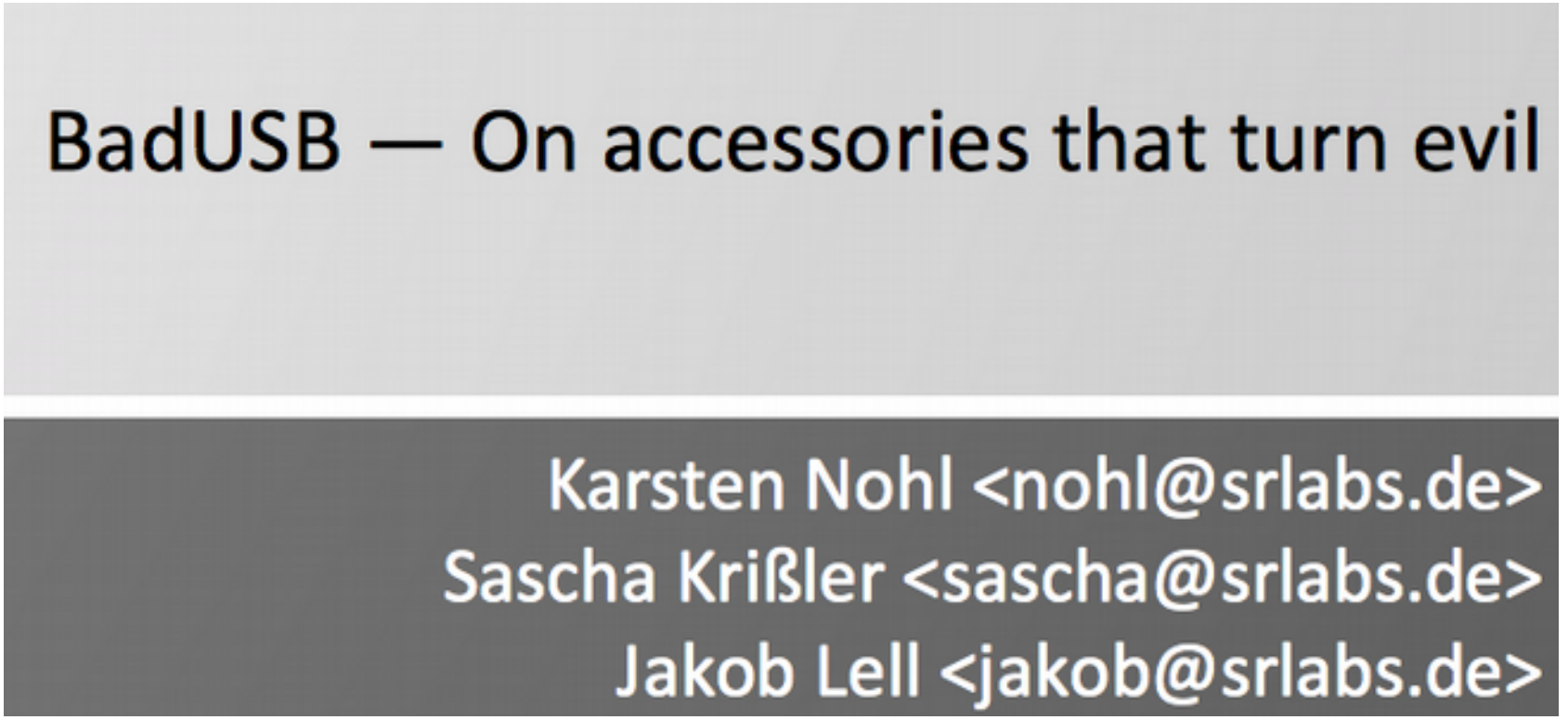
- Empower users with knowledge
- Empower users with informed consent
- Empower users with control over their information – the essence of privacy
- Empower users with verification tools
  - Why can't I verify that the firmware on my apple products actually came from apple?
  - Backdoors aside, we should be able to know if our firmware is from who we think its from
- Make companies even more complicit with mass surveillance if they choose to do so

Why is this important?



Why is this important?

Why is this important?



Why is this Important?

- Empower users with verifiable deletion
- Don't want to have to angle grind our products before disposal
- This is a global problem
- Other work in Central Asia, South America and Africa will benefit from device security
- Internet of things
  - Greater (unknown) digital footprint
  - Greater penetration into our lives
  - Greater problems when things go wrong

Open Questions

- GCHQ doesn't trust Apple devices to keep its secrets – should we?
- When data is more important that national security e.g life and death, how do we delete data?
- How do we know which chips store our sensitive data?
- Do we have a right to know?
- Do we have a right to delete?
- Do we own our devices?

Questions?

- Twitter
  - @musalbas
  - @richietynan
  - @privacyint