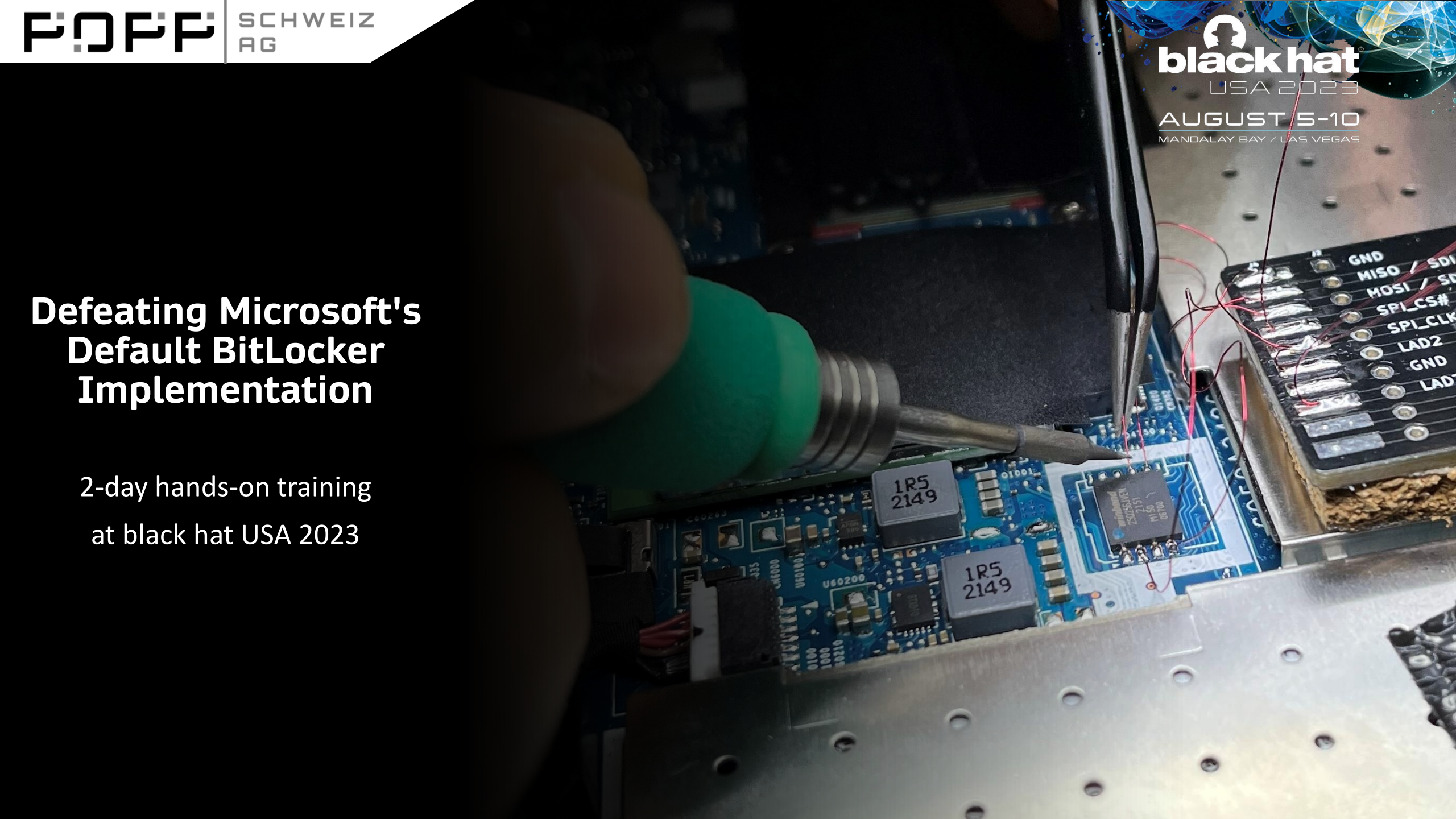
FOFP SCHWEIZ AG



Defeating Microsoft's Default BitLocker Implementation

2-day hands-on training

at black hat USA 2023

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Defeating Microsoft's Default BitLocker Implementation

2-day hands-on training

at black hat USA 2023

Disclaimer

The material presented in this hardware hacking course is intended solely for educational purposes. It is important to understand that the techniques and knowledge acquired here must be used responsibly and within the boundaries of the law. By participating in this course, you acknowledge and agree to the following:

1. The information and skills obtained in this course should only be applied to devices that you own or have obtained legal consent to test.
2. Unauthorized access, disruption, or tampering with any device without appropriate legal consent is strictly prohibited and may result in criminal or civil liability.
3. The instructors and organizers of this course do not condone any illegal or unethical activities, including hacking, that violate the rights and privacy of others.
4. You are solely responsible for any actions you take based on the knowledge gained from this course. The instructors and organizers shall not be held liable for any damages or consequences arising from the misuse or unauthorized application of this knowledge.
5. Always respect the privacy and security of others. Do not attempt to exploit vulnerabilities or compromise the integrity of any device or network without proper authorization.

Remember, hacking can have legal implications, and it is essential to adhere to ethical guidelines and the laws of your jurisdiction.

About Us

Pascal Gujer

- Security Researcher
- BSc Electrical Engineering
- MSc Advanced Cyber Security & Digital Forensics
- Dissertation about TPM & BitLocker

Joel Frei

- Hardware Reverse Engineer
- Electronic Technician
- Flash Memory Forensics
- Maker

Agenda Day 1

- Equipment Inspection
- Soldering Theory & Lab
- Tamper Protection Switches
- Forensic Data Acquisition
- Notebook Internals
- Notebook Disassembly

Key Takeaways

- Ability to Solder
- Tamper Protection Switches
- Basic Forensic Data Acquisition

Agenda Day 2

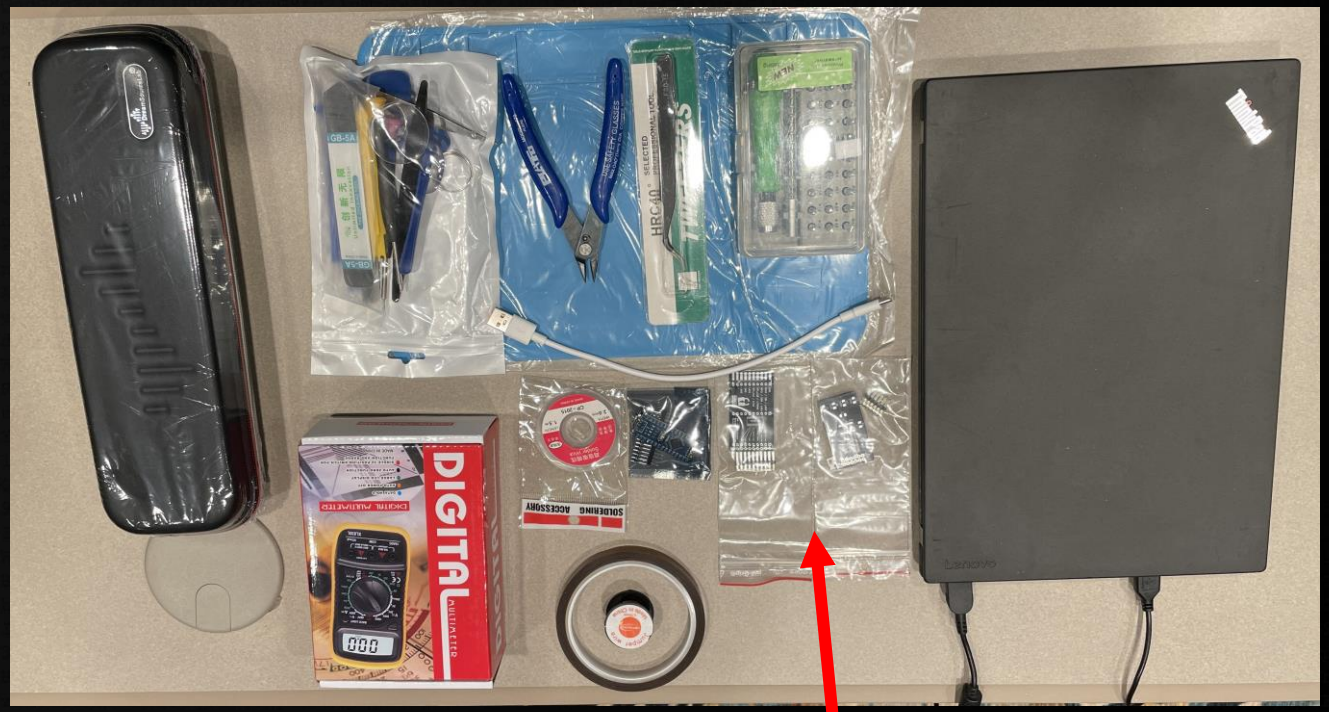
- BitLocker Theory
- TPM Theory
- Soldering to the TPM Bus
- Logic Analyzers & Labs
- Sniffing the Key
- Recovering the Recovery PW
- Extracting Artifacts

Key Takeaways

- BitLocker & TPM Theory
- Logic Analyzers
- Obtaining the Recovery PW

Equipment Inspection

To Keep



To Use

Equipment Inspection

- DSLogic U3Pro16
- Logic Analyzer with

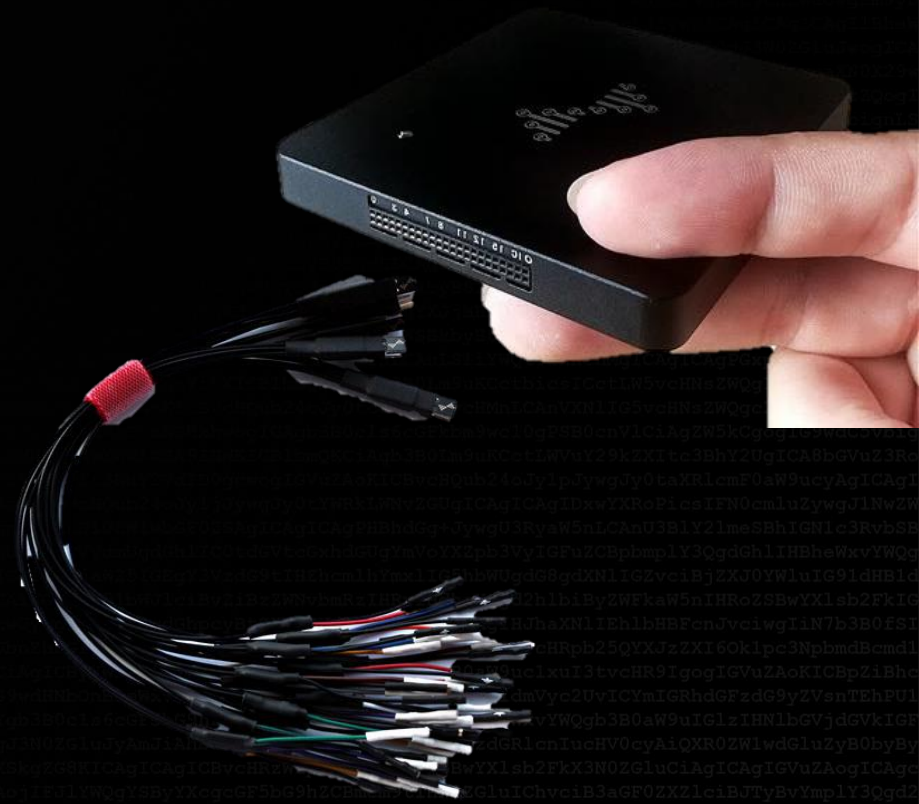
Buffer Mode		Stream Mode	
8 channels:	1 GHz	3 channels:	1 GHz
16 channels:	500 MHz	6 channels:	500 MHz
		12 channels:	250 MHz
		16 channels:	125 MHz

https://www.dreamsourcelab.com/shop/logic-analyzer/dslogic-u3pro16

https://www.dreamsourcelab.com/doc/DSLogic_U3Pro16_Datasheet.pdf

Equipment Inspection

	Direction	Descriptions	Protected Voltage Range
USB 3.0 port	InOut	Connect to host computer	4.75 V ~ 5.25 V
CH0 – CH15	Input	Connect to under test signals	-30 V ~ 30 V
CK	Input	Clock input at state sample mode	0 V ~ 3.3 V (max 50 MHz)
TI	Input	Reserved	0 V ~ 3.3 V
TO	Output	External trigger signal output	n/a



https://www.dreamsourcelab.com/shop/logic-analyzer/dslogic-u3pro16

https://www.dreamsourcelab.com/doc/DSLogic_U3Pro16_Datasheet.pdf

Agenda Day 1

- Equipment Inspection
- Soldering Theory & Lab
- Tamper Protection Switches
- Forensic Data Acquisition
- Notebook Internals
- Notebook Disassembly

Key Takeaways

- Ability to Solder
- Tamper Protection Switches
- Basic Forensic Data Acquisition

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

How to Solder

- Soldering vs. Welding
- SMD vs. THT
- Solder Wire Alloys
- Solder Wire
- Flux
- Solder Iron
- Solder Instructions
- Solder Joints
- Coated Wires
- Tips and Tricks
- Practical Soldering

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Soldering vs. Welding

How to Solder

- Soldering
  - Only the solder is melting during the solder process
  - Soft soldering (194 °F – 842 °F)
  - Hard soldering (842 °F – X)

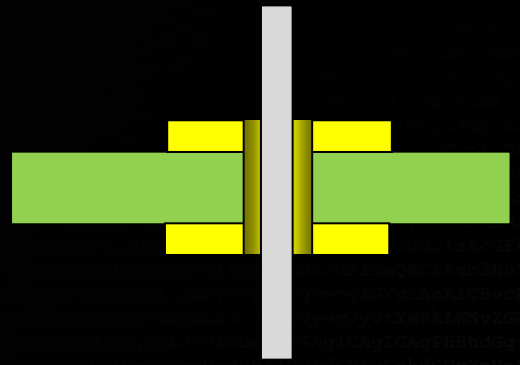
- Welding
  - Much higher temperature
  - All work pieces are melting together

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

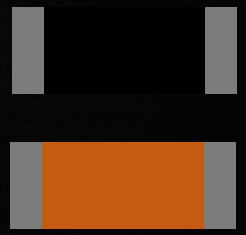
SMD vs. THT

How to Solder

- **THT (through-hole technology)**



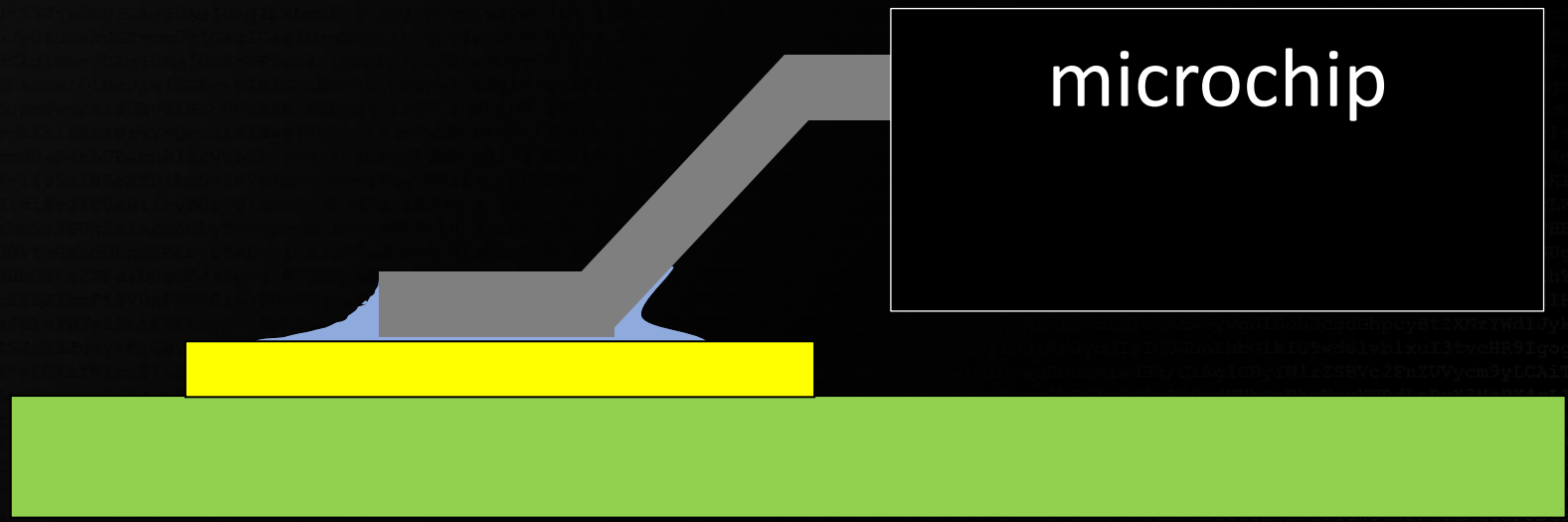
- **SMD (surface-mounted device)**



SMD vs. THT

How to Solder

- Micro-Soldering
  - It’s the same as THT soldering just a “little bit” smaller ;-)



black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Solder Wire Alloys

How to Solder

- Material for solder wires

Element	Symbol	Melting Temp.	Specials
Tin	Sn	449.6 °F	Main component of soft solders
Lead	Pb	621.5 °F	Reduction of the melting temperature of the solder, **improvement of the flow properties**
Bismuth	Bi	520.34 °F	Significant reduction in melting temperature of the solder
Antimon	Sb	1167.26 °F	Increases the tensile strength of the solder, reduces the amount of shrinkage
Silver	Ag	1763.42 °F	reduces the alloying of silver from the workpieces or electronic components
Copper	Cu	1983.92 °F	reduces the alloying of copper from the workpieces or electronic components; extends the life of soldering tips

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Solder Wire Alloys

How to Solder

- Eutectic ?!
- Example with SnPb Solder

solid	pap	fluid	
50 / 50 solder	361 °F	420.8 °F	
solid	pap	fluid	
55 / 45 solder	361 °F	375 °F	
solid	fluid		
63 / 37 solder	361 °F -> eutectic		

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Solder Wire Alloys

How to Solder

Alloy	Temperature (°F)		Remarks	Application
	Solid	Liquid		
Sn63Pb37	361.4 °F	361.4 °F	Eutectic	Old Standard Solder
Sn42Bi58	280.4 °F	280.4 °F	Eutectic	Low Temperature Solder
Sn96.5Ag3.0Cu0.5	422.6 °F	426.2 °F	"SAC305"	Leadfree Solder
Sn96Ag4(Sn96.3Ag3.7)	429.8 °F	429.8 °F	Eutectic	Leadfree Solder
Sn99.3Cu0.7	440.6 °F	440.6 °F	Eutectic	Leadfree Solder
Au80Sn20	536.0 °F	536.0 °F	Eutectic	Chip bonding

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Solder Wire

How to Solder

- Lead-free vs leaded solder wire
- SnPb solder wire
  - Very good flow properties
  - Lower melting temperature
  - Perfect eutectic
  - Cheap

- Easy to solder ☺
- Forbidden for most cases in industrial production ☹

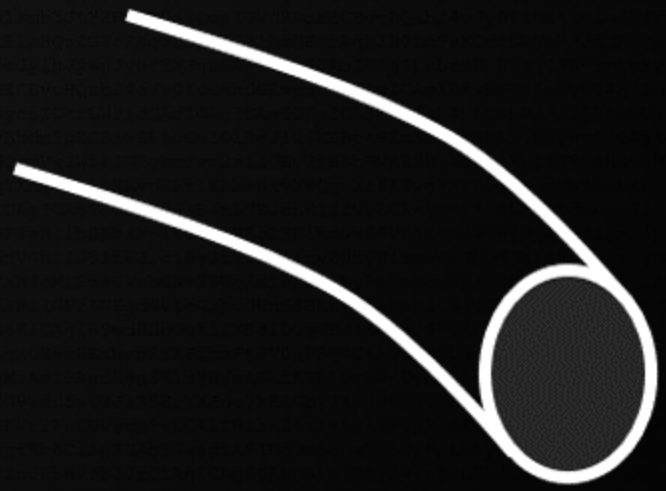
- Sn99.3Cu0.7 solder wire
  - Poor flow properties
  - wetting slowly
  - More expensive
  - Needs more Flux

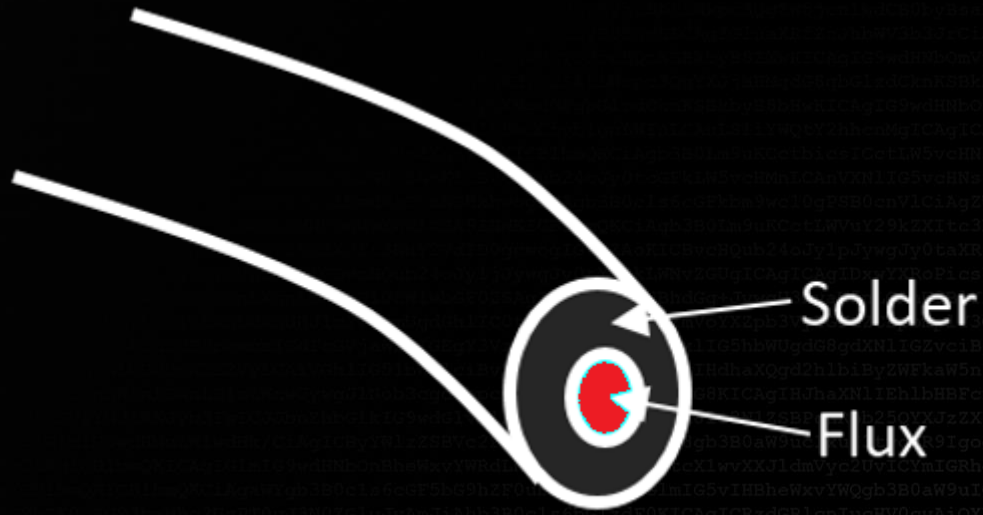
- The new standard in industrial production ☺
- Harder to solder ☹

Solder Wire

How to Solder

- Types of solder wire





black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Flux (Latin Fluxus => Flow)

How to Solder

- Material
  - Natural rosin (from pine trees)
  - Other additives to improve some characteristics
- Rosin flux grades (grade of activity: **L** = low, **M** = moderate, **H** = high)

- **R** (Rosin) – pure rosin, no activators, low activity, mildest
- **WW** (water-white) – purest rosin grade, no activators, low activity, sometimes synonymous with R
- **RMA** (rosin mildly activated) - contains mild activators, typically no halides
- **RA** (rosin activated) – rosin with strong activators, high activity, contains halides
- **OA** (organic acid) – rosin activated with organic acids, high activity, highly corrosive, aqueous cleaning
- **SA** (synthetically activated) – rosin with strong synthetic activators, high activity; formulated to be easily soluble in organic solvents (chlorofluorocarbons, alcohols) to facilitate cleaning
- **WS** (water-soluble) – usually based on inorganic or organic halides; highly corrosive residues
- **SRA** (superactivated rosin) – rosin with very strong activators, very high activity
- **IA** (inorganic acid) – rosin activated with inorganic acids (usually hydrochloric acid or phosphoric acid), highest activities, highly corrosive

R, WW, and RMA grades are used for joints that can not be easily cleaned or where there is too high corrosion risk. More active grades require thorough cleaning of the residues. Improper cleaning can actually aggravate the corrosion by releasing trapped activators from the flux residues.

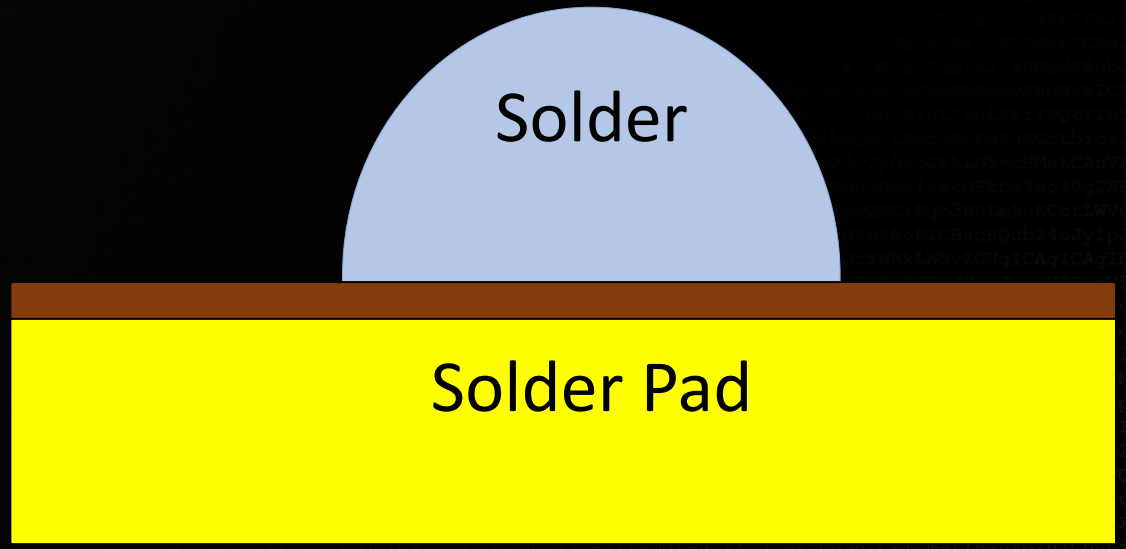
https://en.wikipedia.org/wiki/Flux_(metallurgy)#Rosinfluxes

Flux

How to Solder

- Oxidation is the enemy of a good solder point

Oxidation Layer

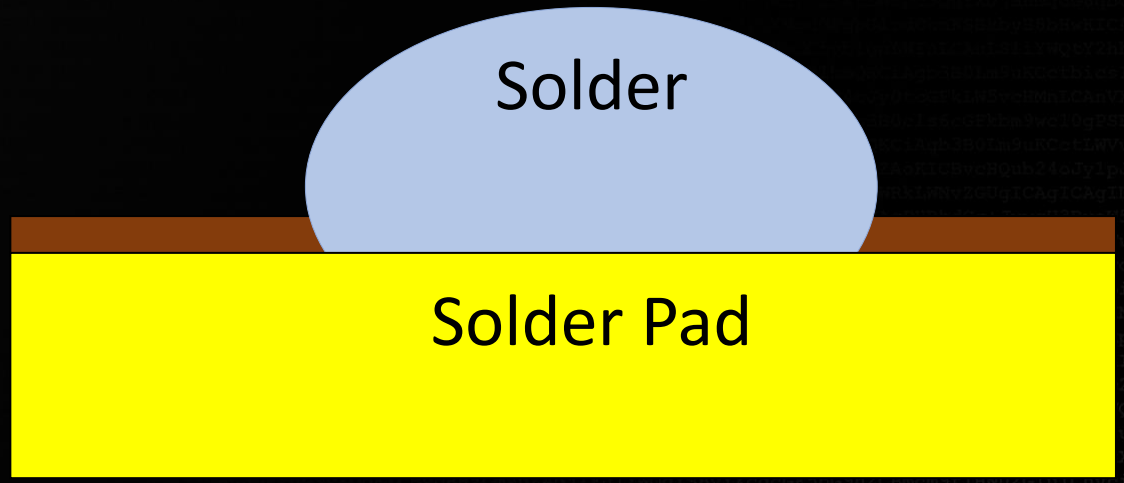


Flux

How to Solder

- Removes oxide films from the surface of the solder pad
- Increases the wetting ability of the solder

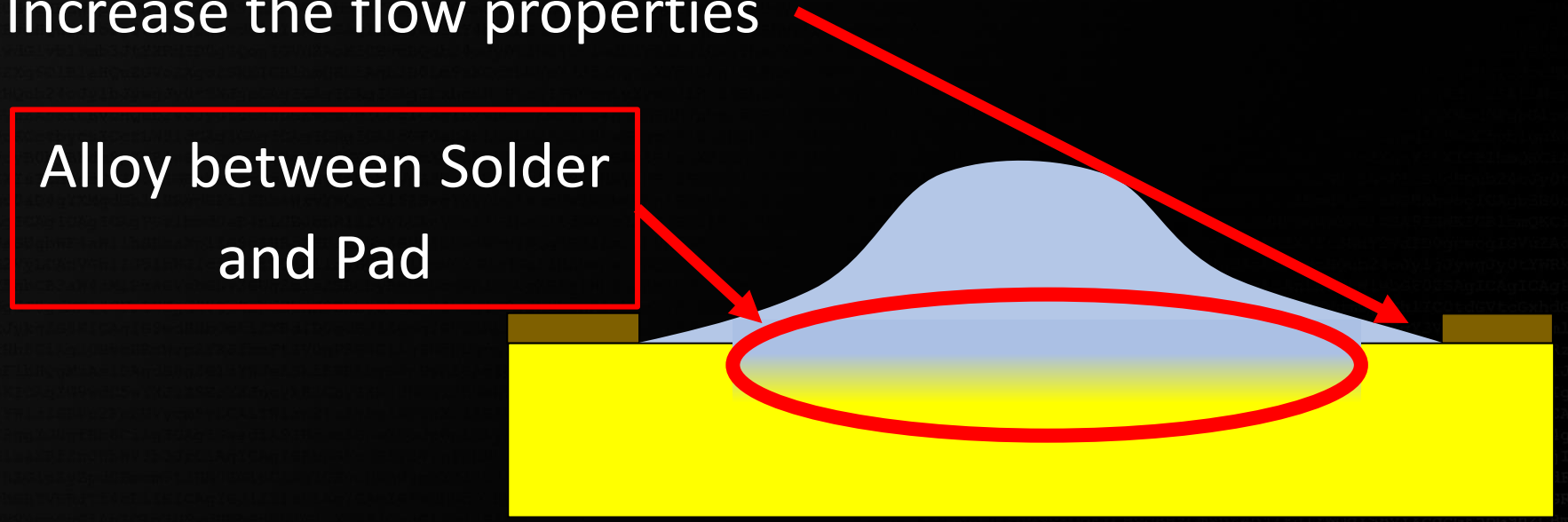
Oxidation Layer



Flux

How to Solder

- Copper and solder can form a good alloy in the boundary layer
- Increase the flow properties

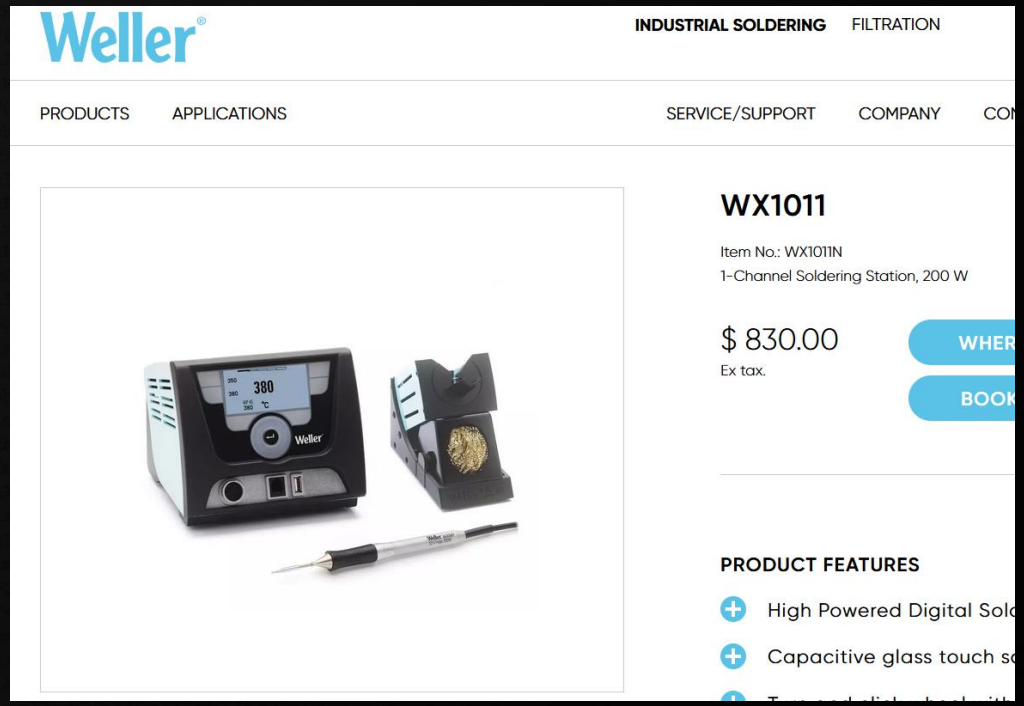


black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Solder Iron

How to Solder

- Solder Station - the Expensive



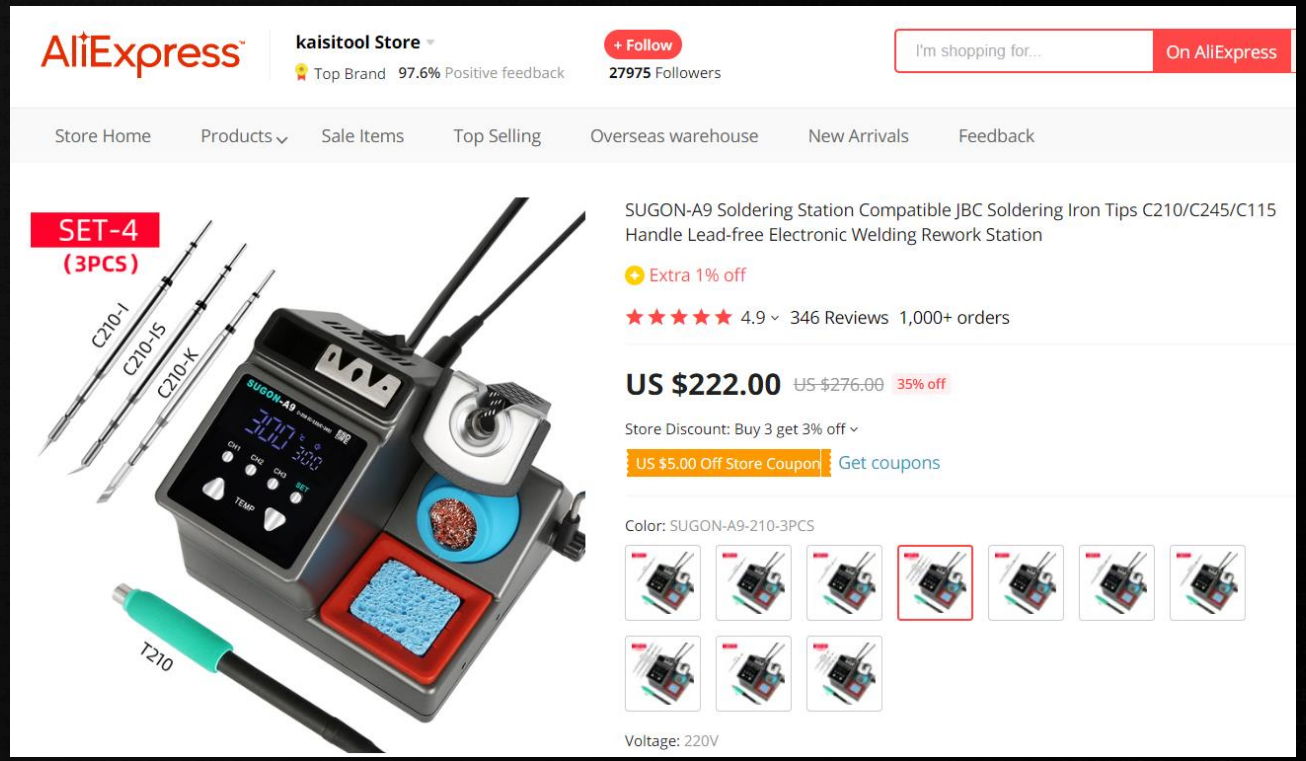
JBC
CDE-1BQA
ca. 600 USD

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Solder Iron

How to Solder

- Solder Station - the Cheaper and Good ~200 USD



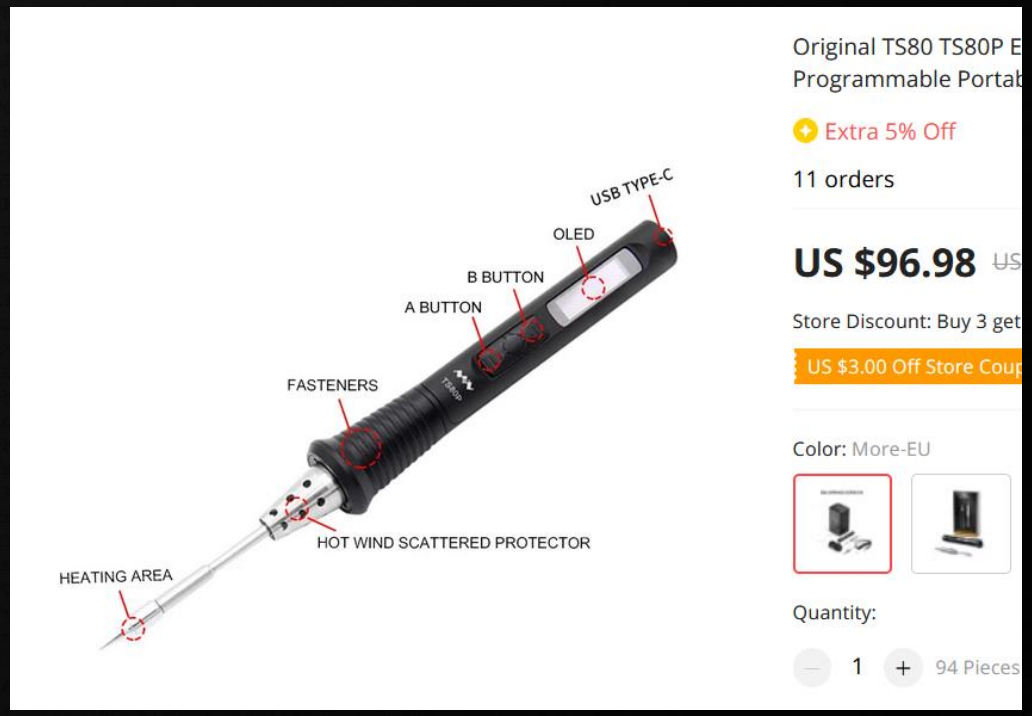
SUGON-A9

https://s.click.aliexpress.com/e/_m0QAjqE

Solder Iron

How to Solder

- Solder Iron – the Mobile one for use with a power bank



TS80P

https://s.click.aliexpress.com/e/_mq0o7du

Xtorm XB303

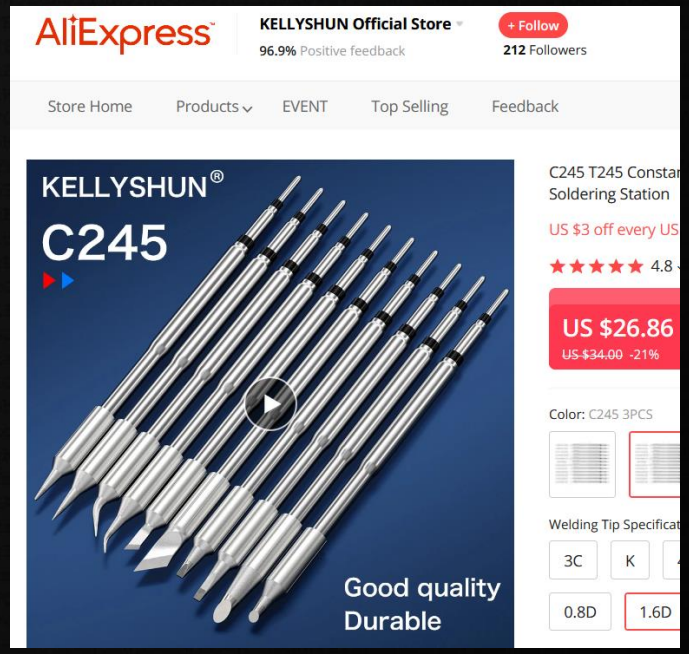
2600 mAh, 60 W

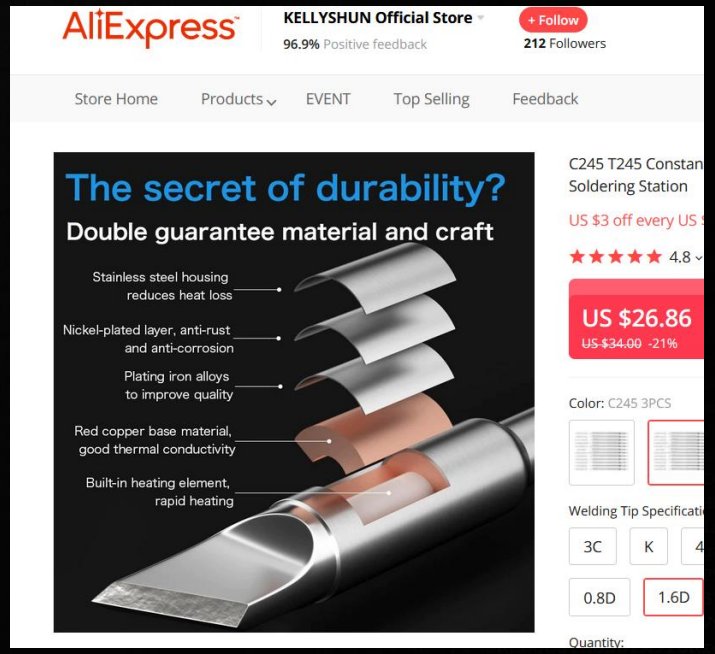
black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

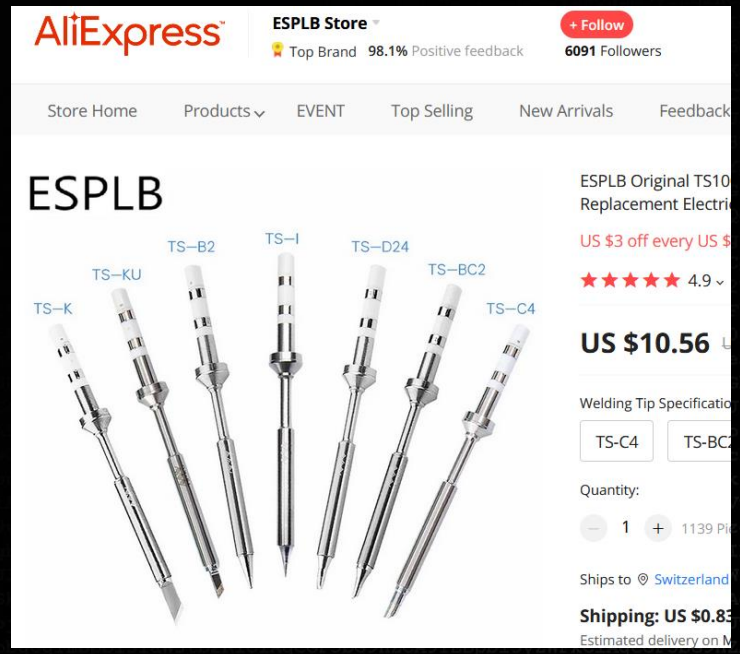
Solder Iron

How to Solder

- The better the solder tip, the easier to solder





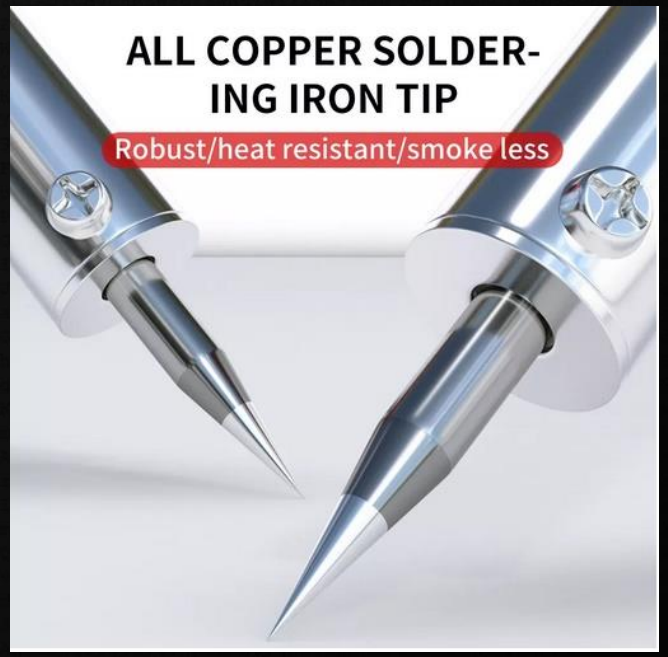


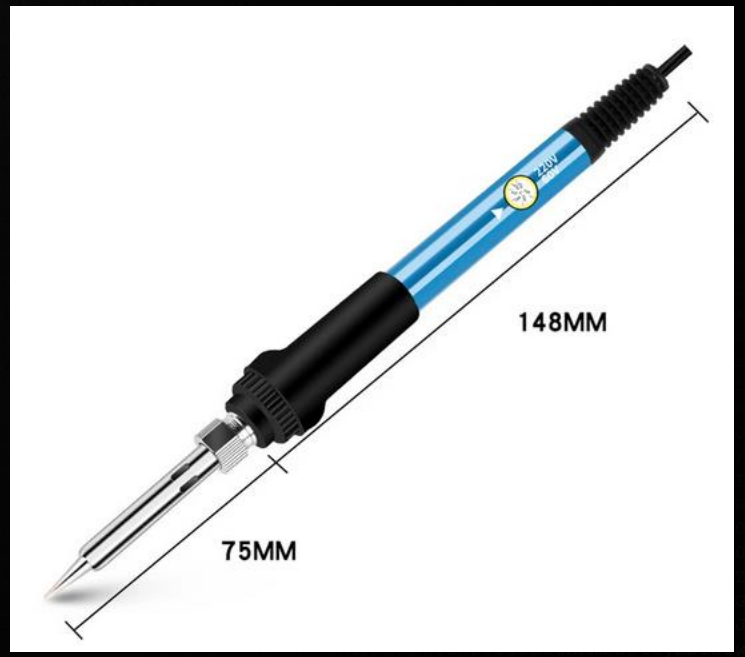
black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Solder Iron

How to Solder

- Solder tip should be one piece from electronic to tip





black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Solder Iron

How to Solder

- Use always the biggest Solder-Tip you can!!!

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Solder Iron

How to Solder

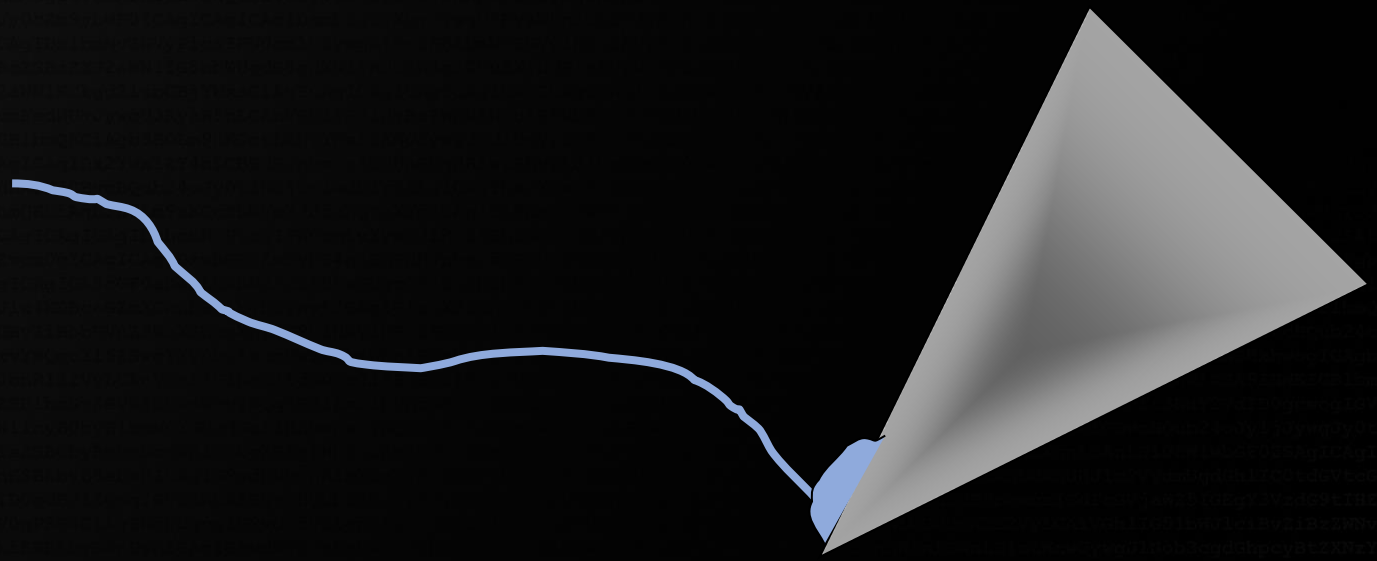
- Minimum Tip temperature:
  - Lead free solder: 662 °F
  - Leaded solder: 410 °F
  - Burn away isolation from coated wire: ≥ 644 °F

- Too hot Tip temperature increases the wear of the tip
  - Our Solder Station reduces the temperature automatically if it is not in use ☺

Solder Instructions

How to Solder

- Step 1

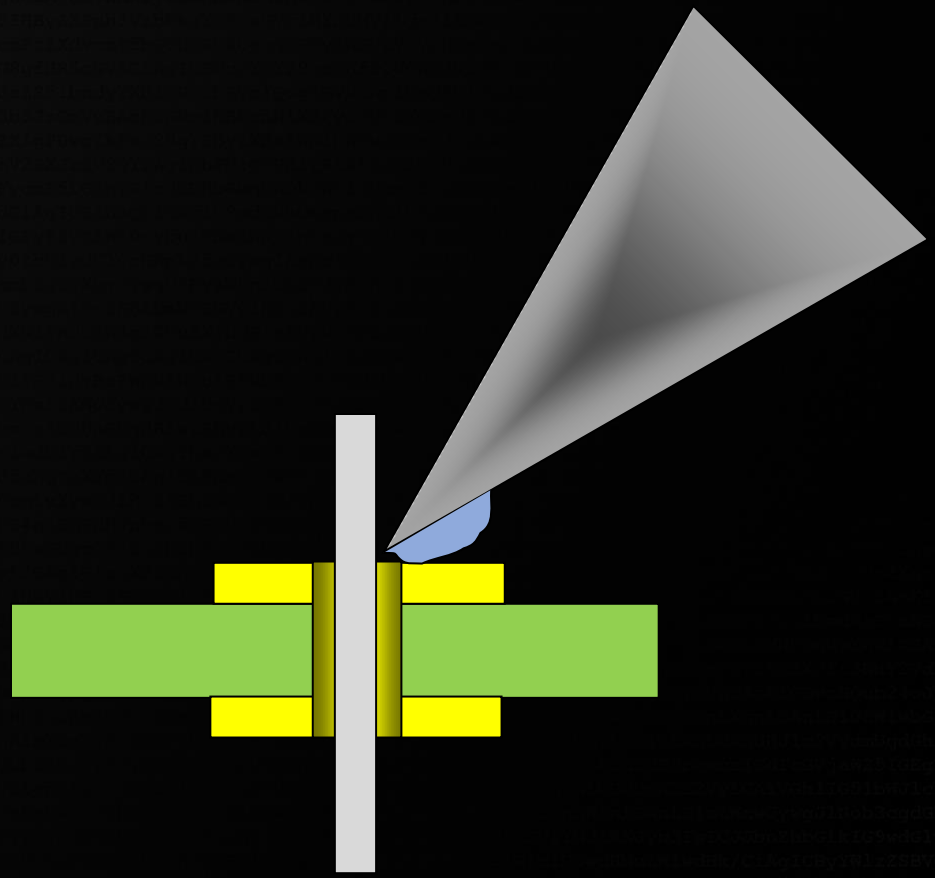


Clean your Solder Iron and put a small amount of solder on it

Solder Instructions

How to Solder

- Step 2

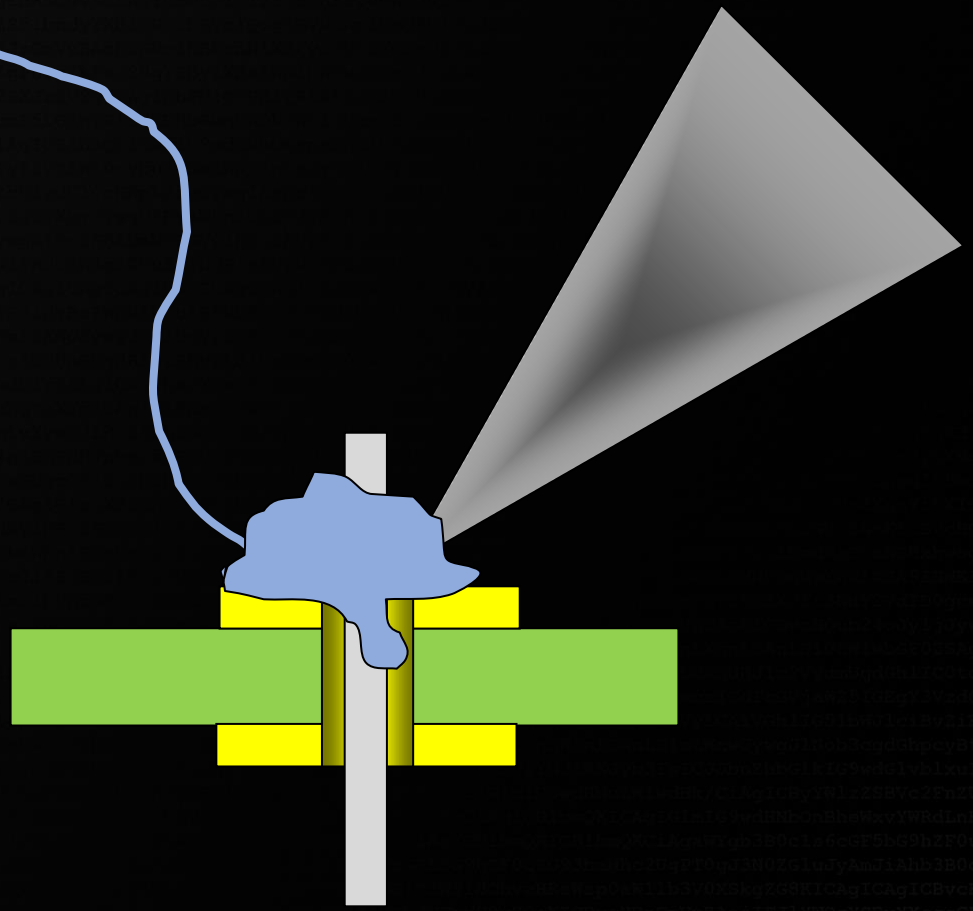


Heat the solder pad on the PCB and the wire
Wait for a second or two

Solder Instructions

How to Solder

- Step 3



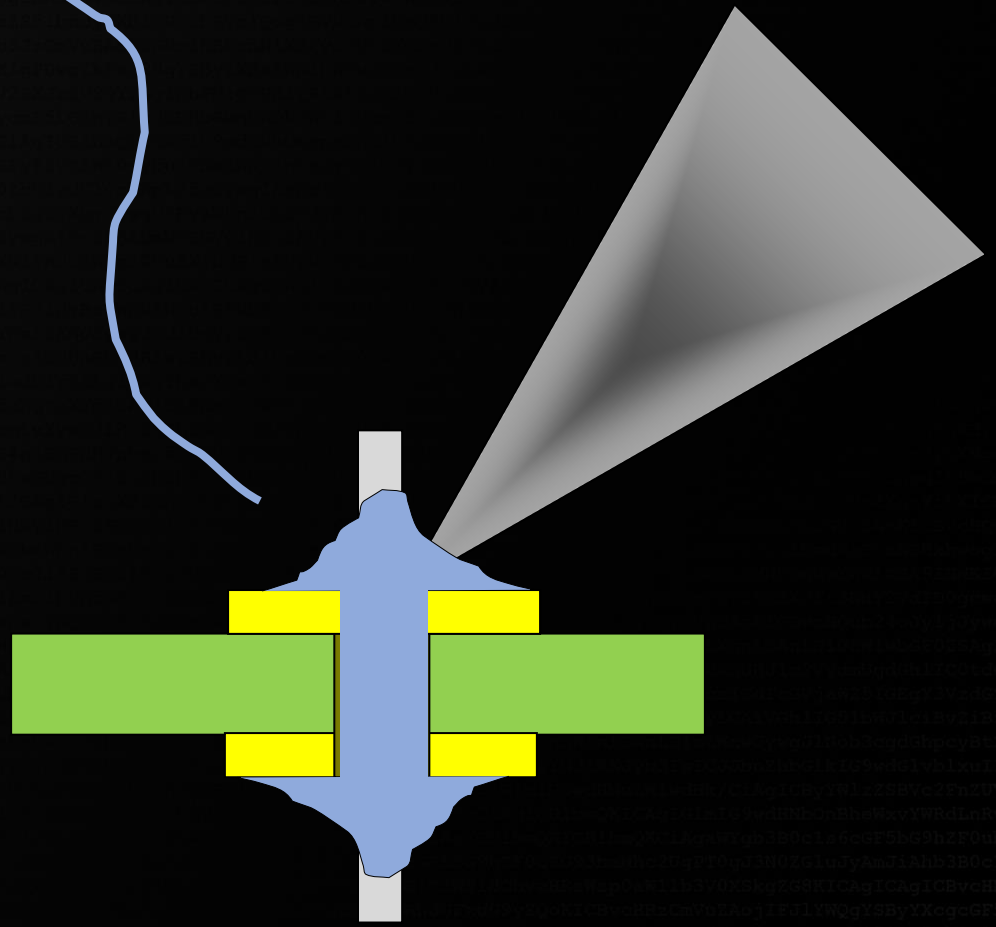
Insert solder

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Solder Instructions

How to Solder

- Step 4



Wait until solder flows through the hole

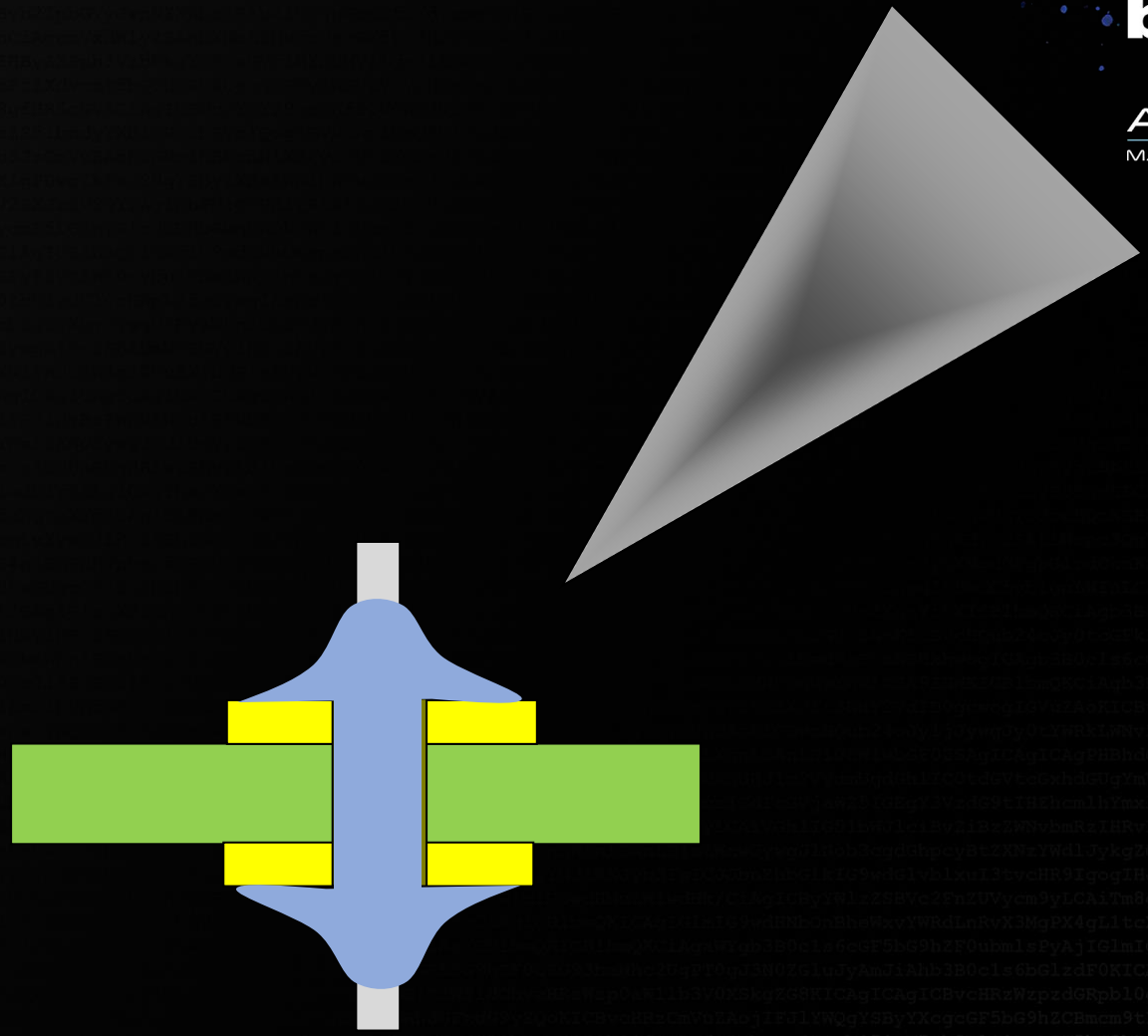
Pull out solder

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Solder Instructions

How to Solder

- Step 5



Pull out solder iron

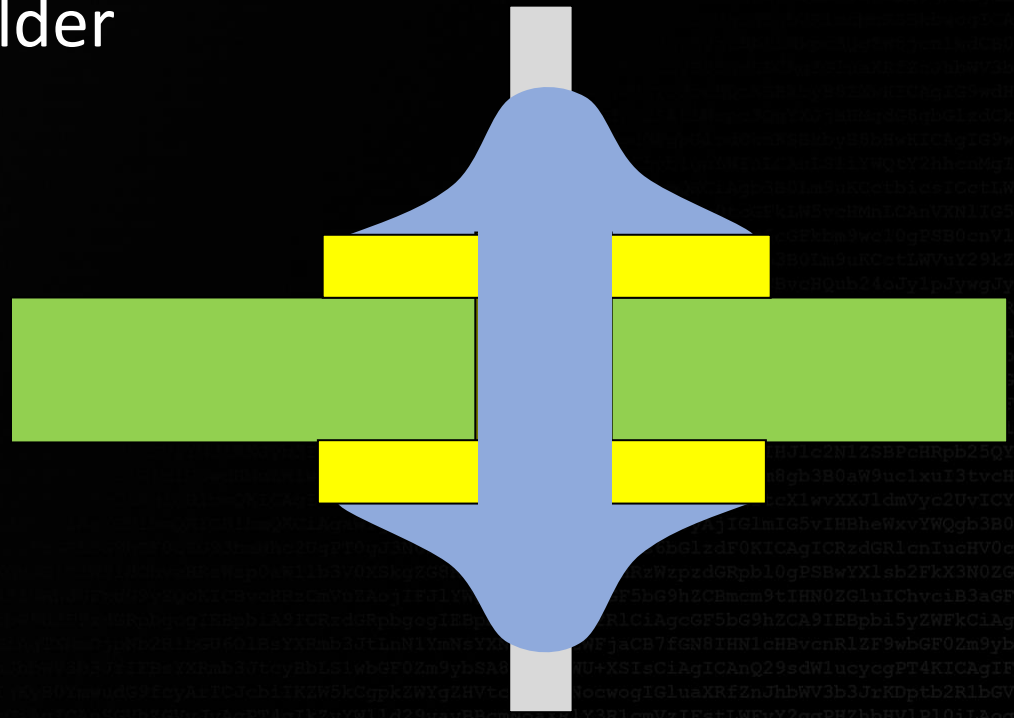
black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Solder Joints

How to Solder

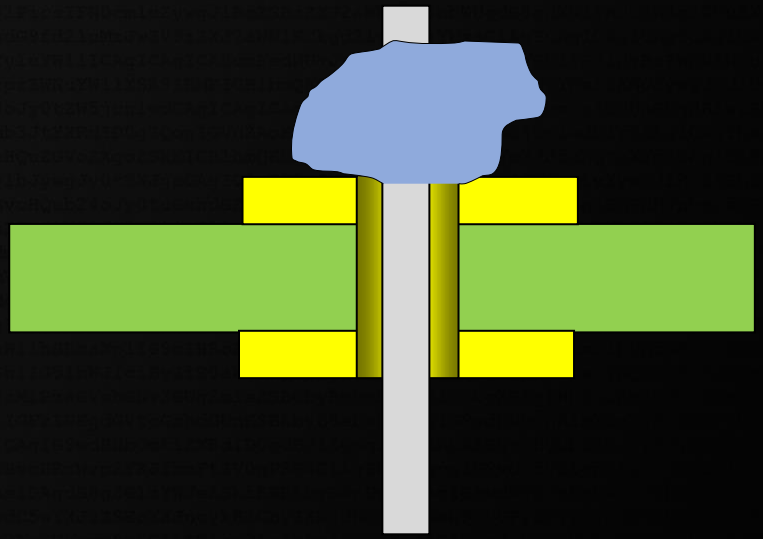
- The hole is filled with solder
- The surface is well wetted with solder
- The surface is smooth and glossy
- The surface has a concave bow

→ A good solder joint!



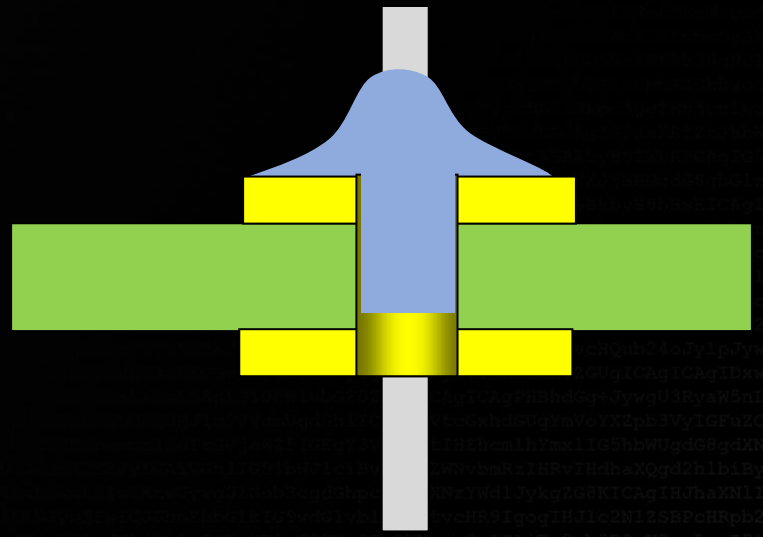
Solder Joints

How to Solder



Not long enough heated

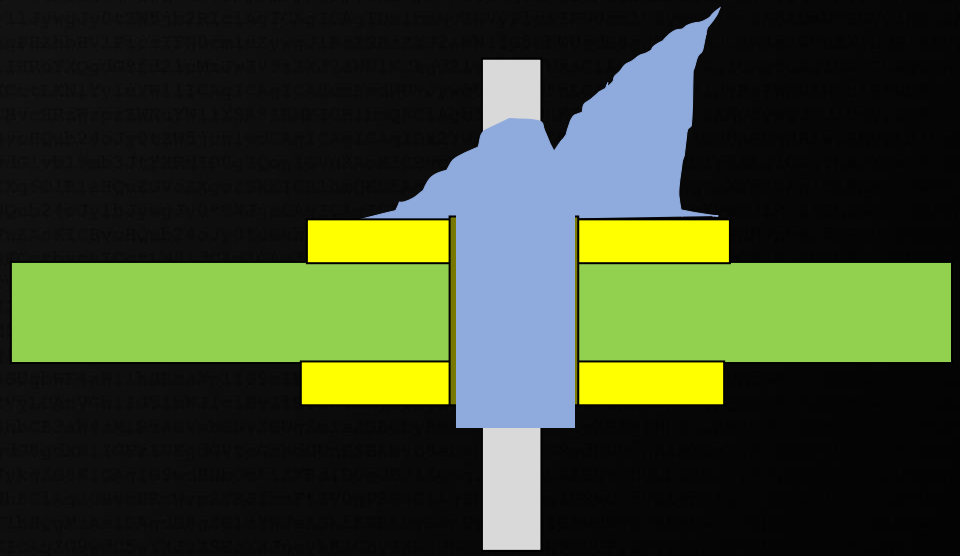
possibly more flux



Not enough solder

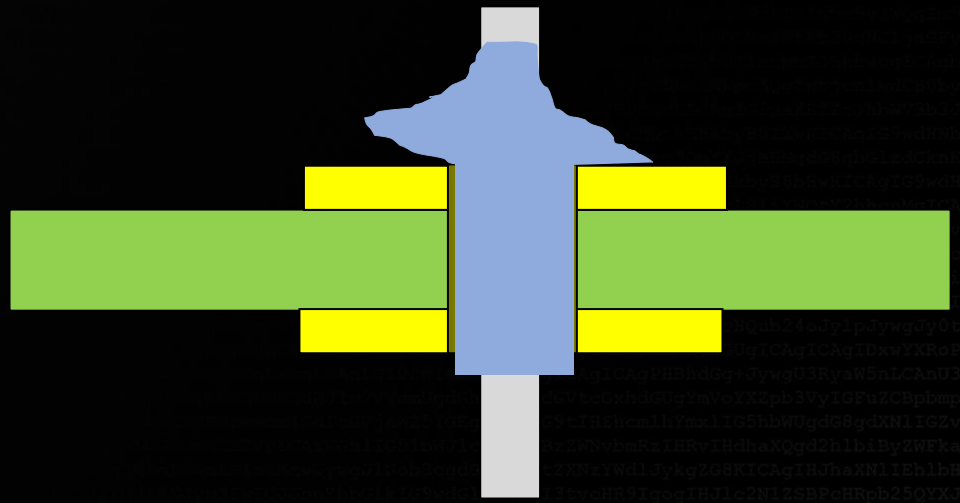
Solder Joints

How to Solder



Not long enough heated

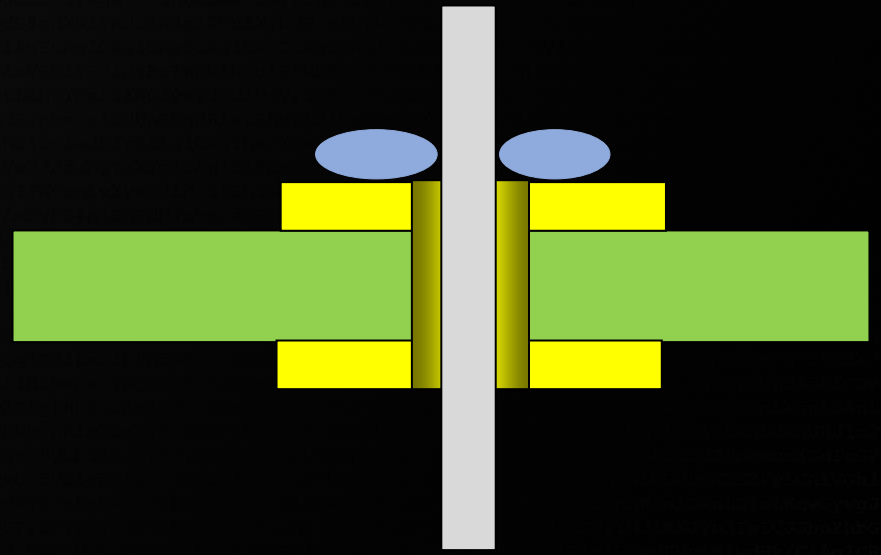
possibly more flux



Not enough solder

Solder Joints

How to Solder



Not enough solder

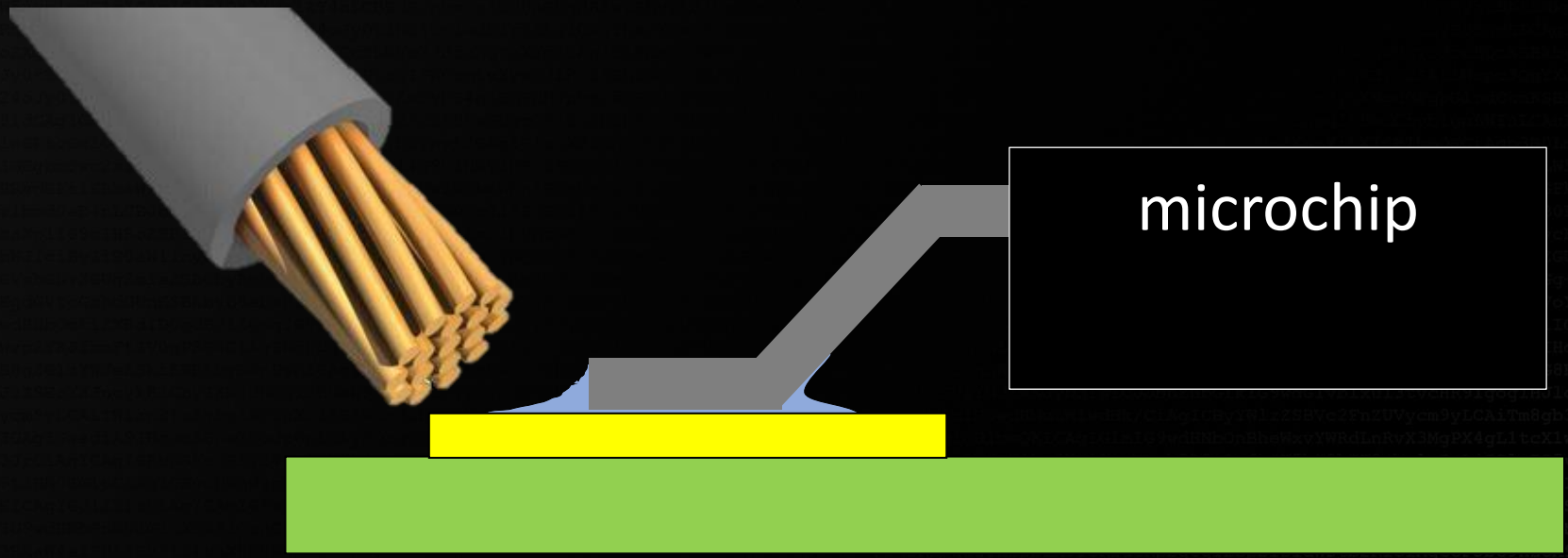
More time for heating

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Coated Wires

How to Solder

- Normal strand wire is too big for soldering on microchips



black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Coated Wires

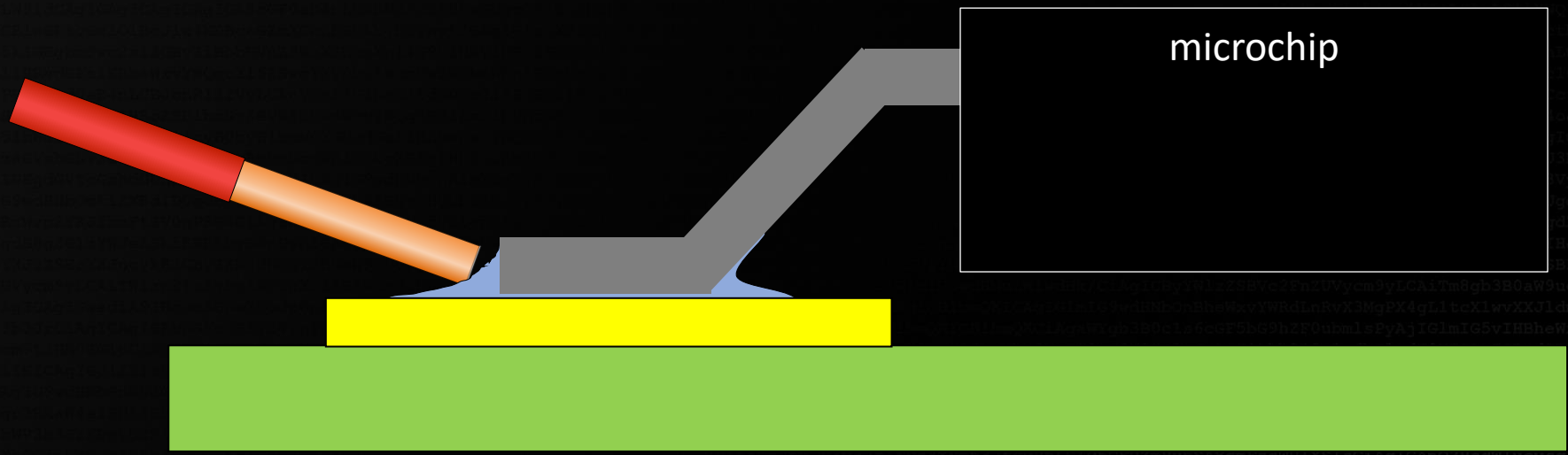
How to Solder

- We need something smaller: coated wire
- Benefits:
  - Very thin wires down to 0.04 mm
  - The coating is electrically insulating

Coated Wires

How to Solder

- Thin and flexible enough for soldering on microchips or tracks on the PCB

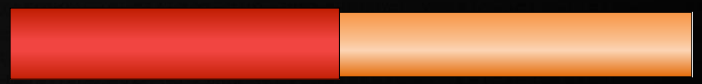


black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Coated Wires

How to Solder

- Remove the coating:
  - **<u>Use your solder iron with a big tip</u>**
  - Min. temperature: 644 °F
  - Use Flux
  - More solder
  - More Flux (flux is inside the solder)

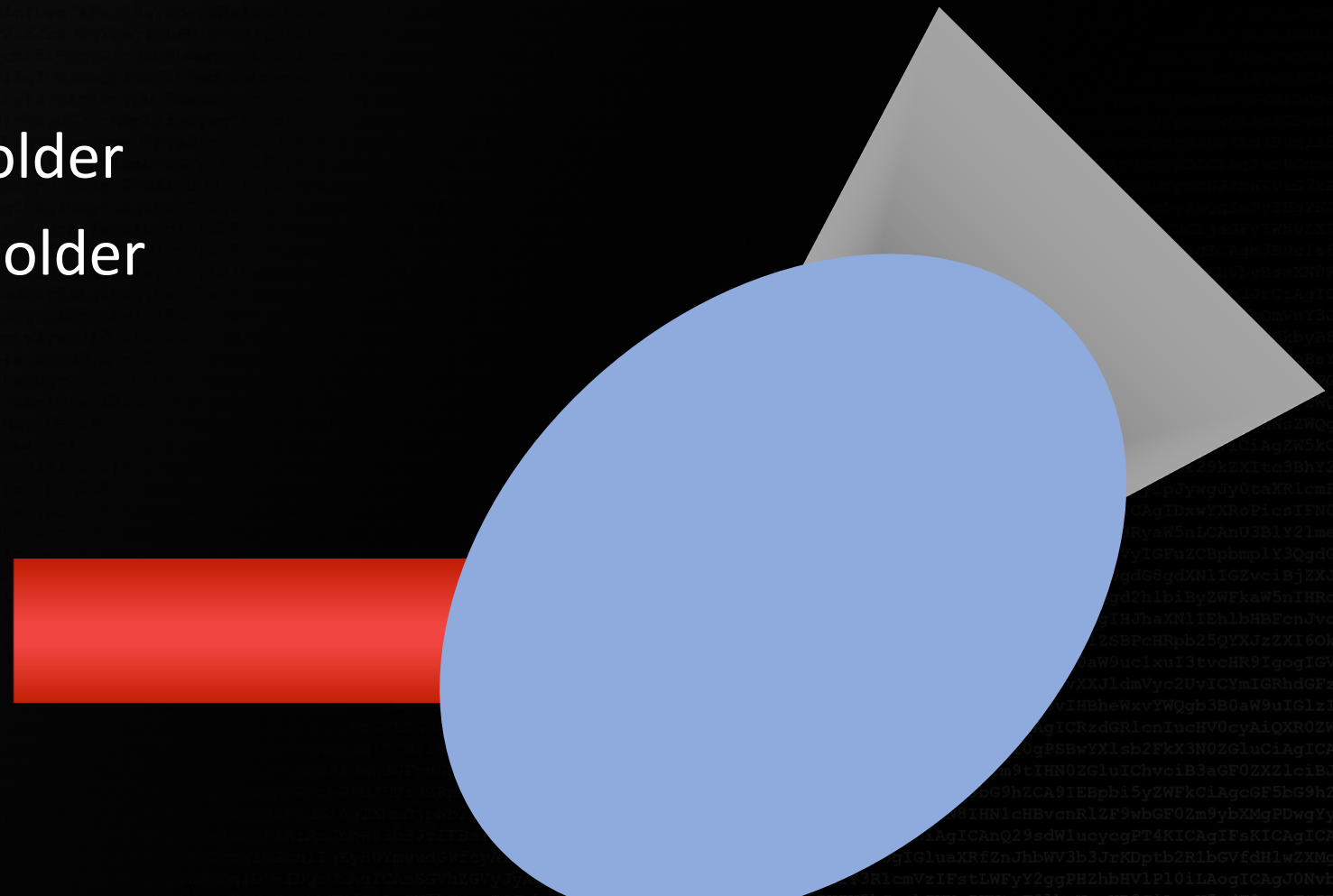


black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Coated Wires

How to Solder

- Melt a large drop of solder
- Dip the wire into the solder
- Wait some seconds

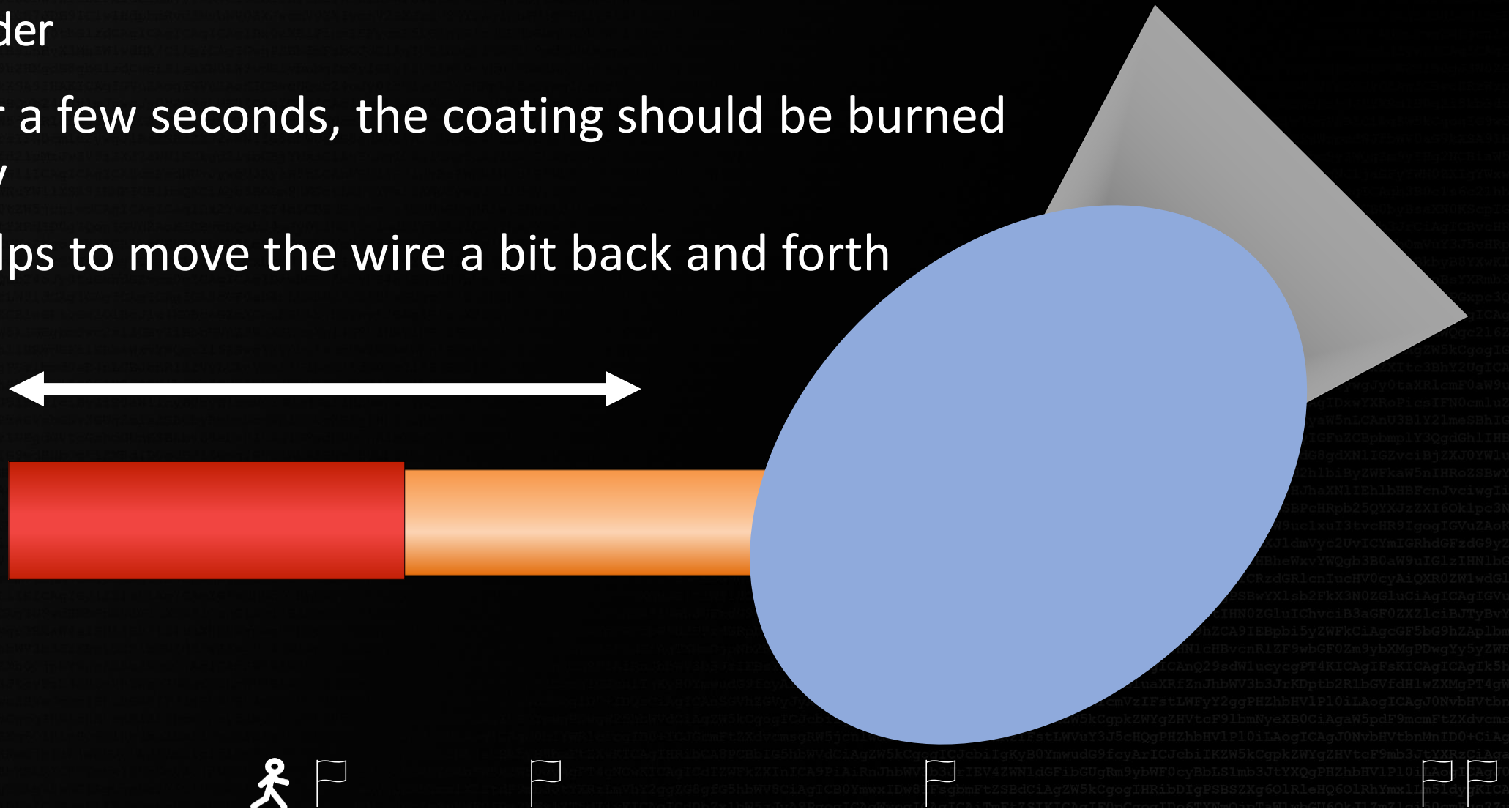


black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Coated Wires

How to Solder

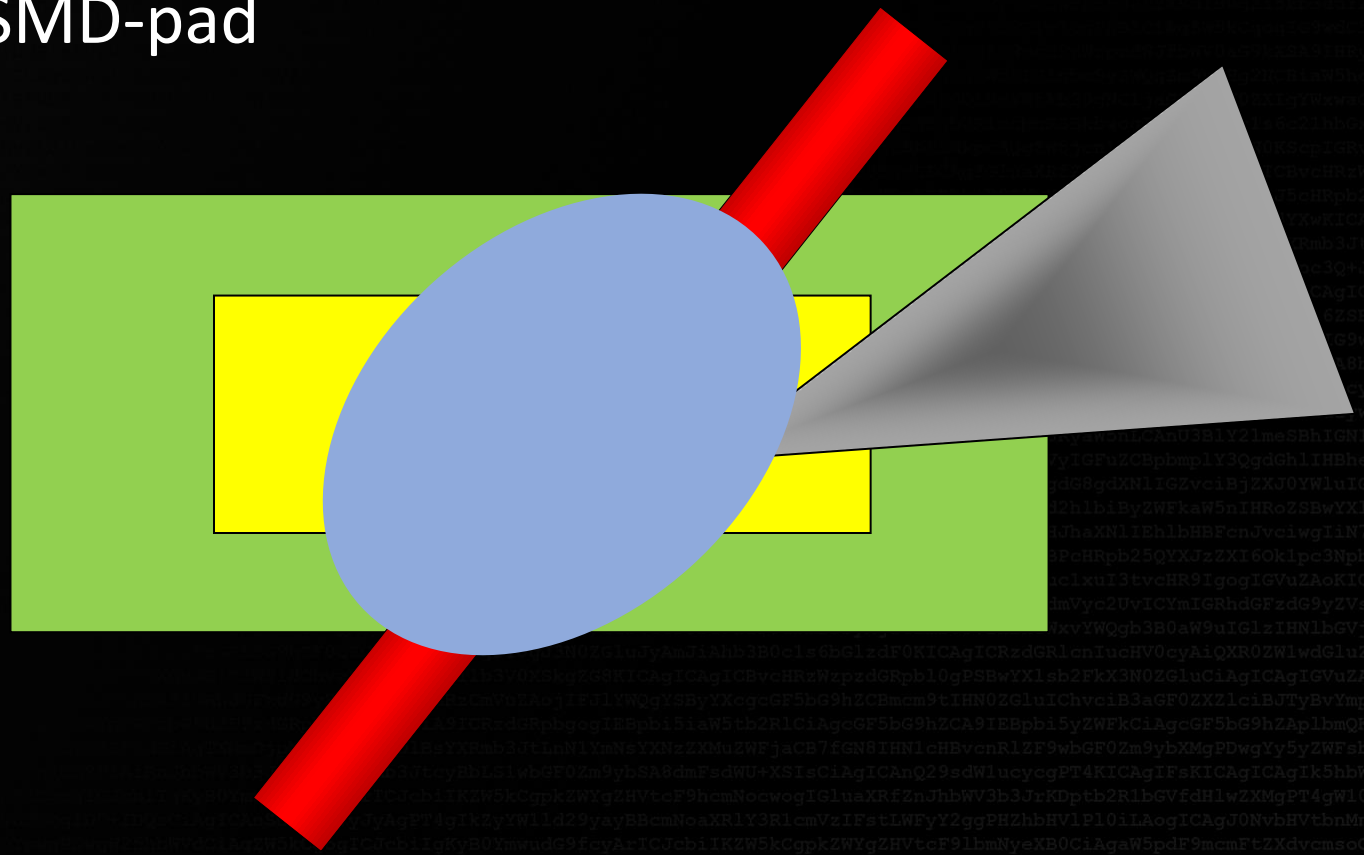
- After a few seconds, the coating should be burned away
- It helps to move the wire a bit back and forth



Coated Wires

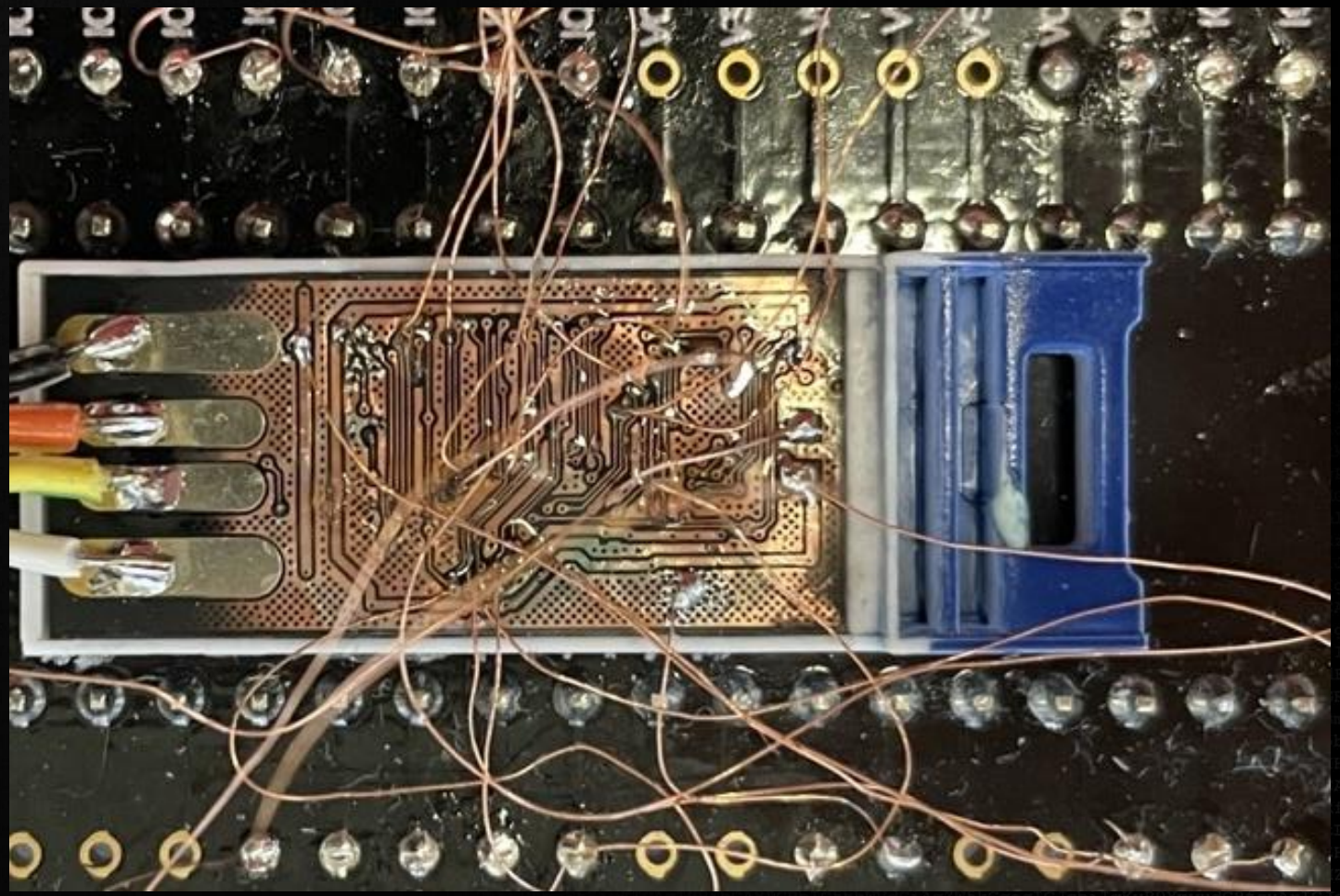
How to Solder

- How to Remove Coating on SMD-pad
  - Pre-tin the pad
  - Use Flux!
  - Take your time
  - After removing the coating just break the ongoing wire away



Soldering directly to PCB Tracks

Interjection



black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Tips and Tricks

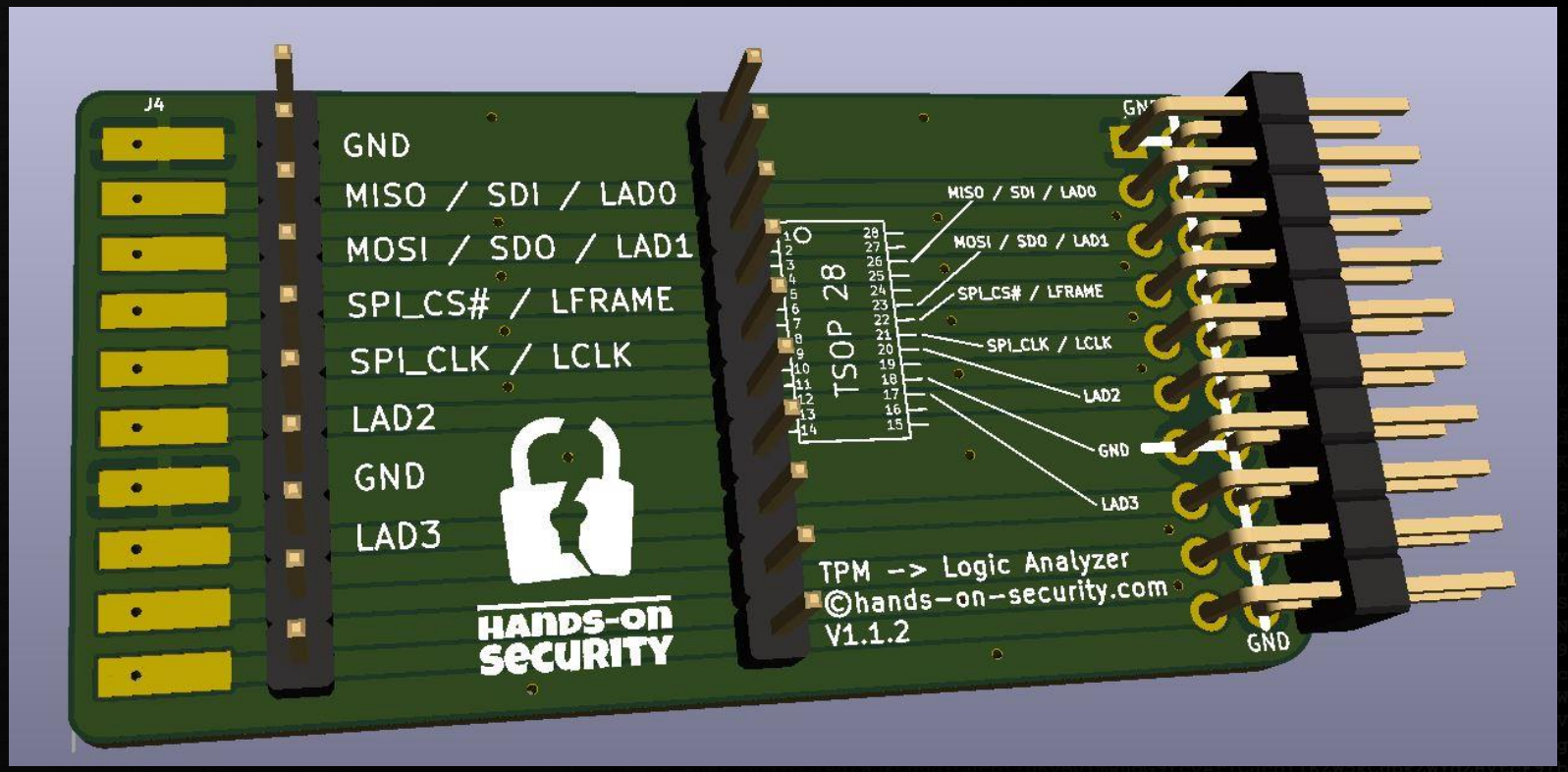
How to Solder

- Always use the **biggest Solder tip** you can.
  - The bigger, the more energy is saved in the tip and the faster you can heat up the components and Pad.
- Use **flux** for micro-soldering, it makes it so much easier
- If you are allowed use Sn63**Pb**37 solder, it's much easier to solder as with lead-free solder
- Use thin solder wire for micro-soldering
- Take your time!
- If the solder is sticky use Flux ;-)

Practical Soldering Warm Up 1

How to Solder

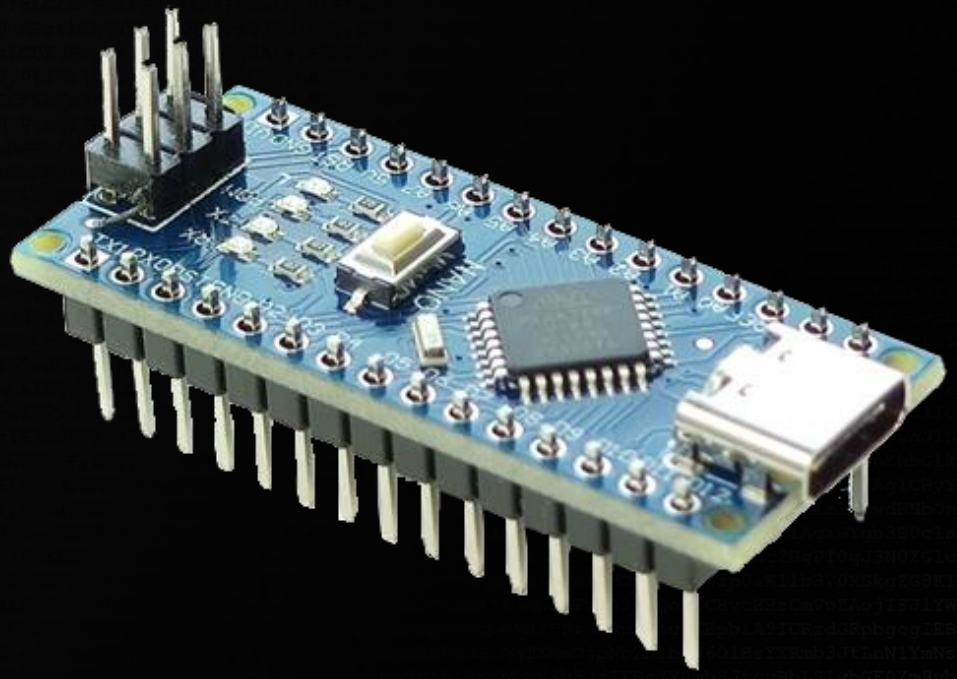
- Solder your own TPM Attack Adapter Board



Practical Soldering Warm Up 2

How to Solder

- Solder the Bus Sniffing Demo Device



CANADUINO® Arduino NANO V3 USB-C Atmega328P + CH340

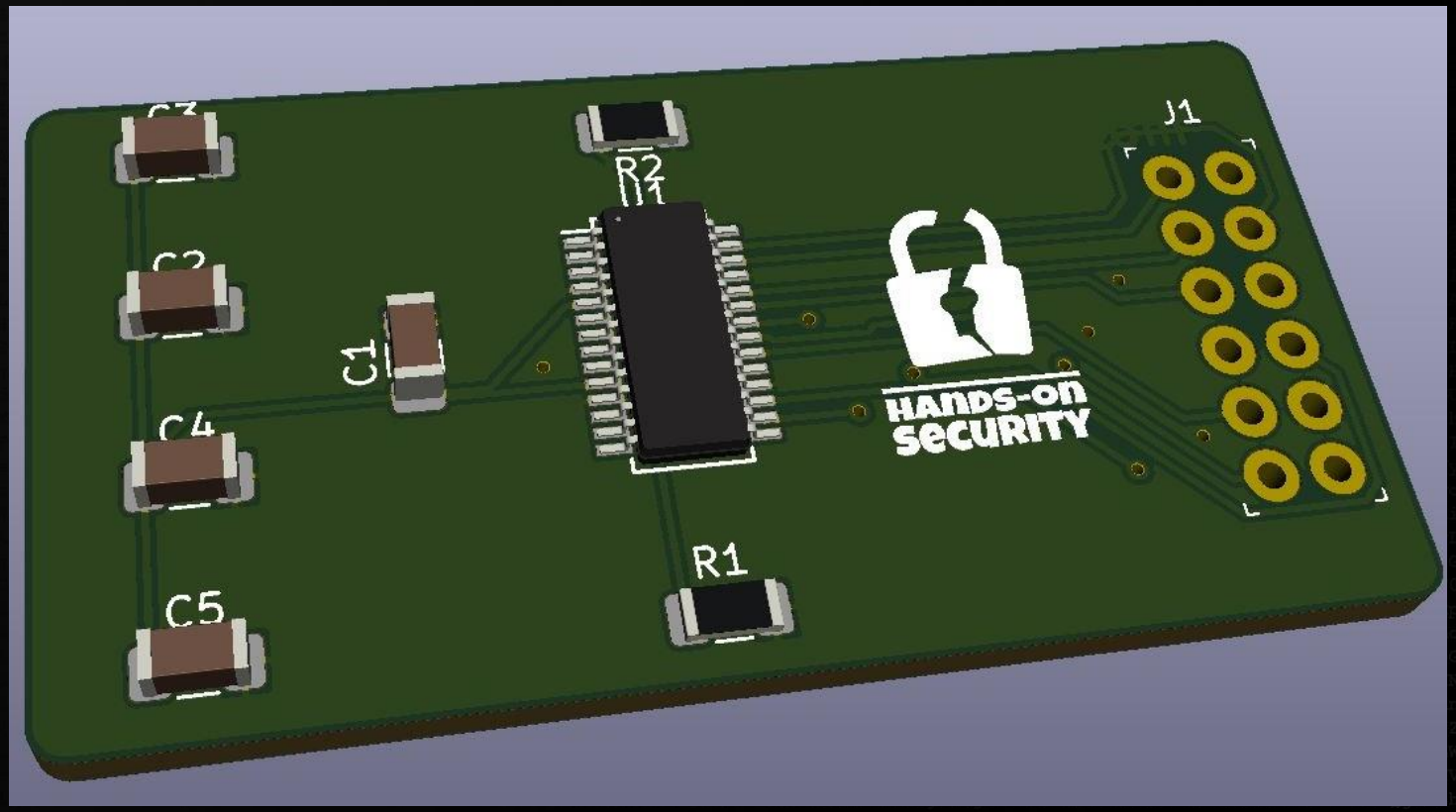
black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Coffee Break

Practical Micro-Soldering

How to Solder

- Solder your own TPM Board (compatible with certain gigabyte mainboards)



Agenda Day 1

- Equipment Inspection
- Soldering Theory & Lab
  - Tamper Protection Switches
  - Forensic Data Acquisition
  - Notebook Internals
  - Notebook Disassembly

Key Takeaways

- Ability to Solder
  - Tamper Protection Switches
  - Basic Forensic Data Acquisition

Lunch Break

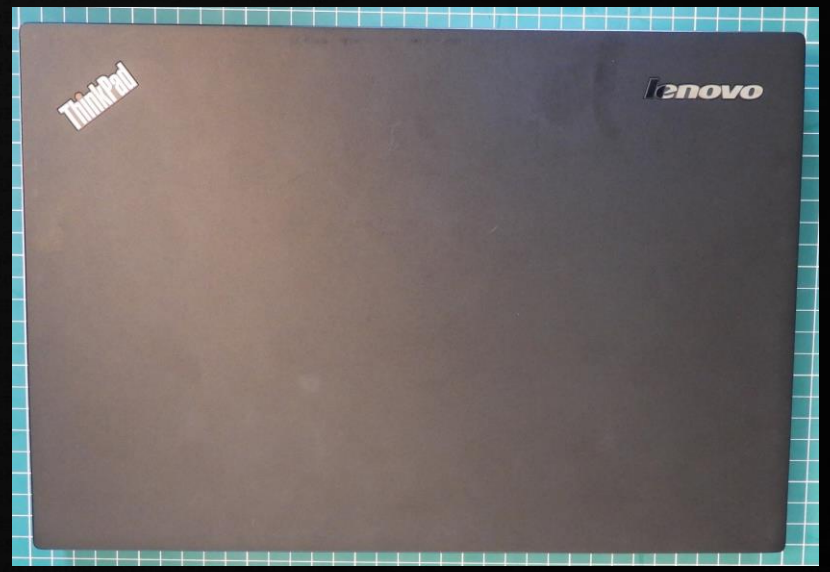
black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

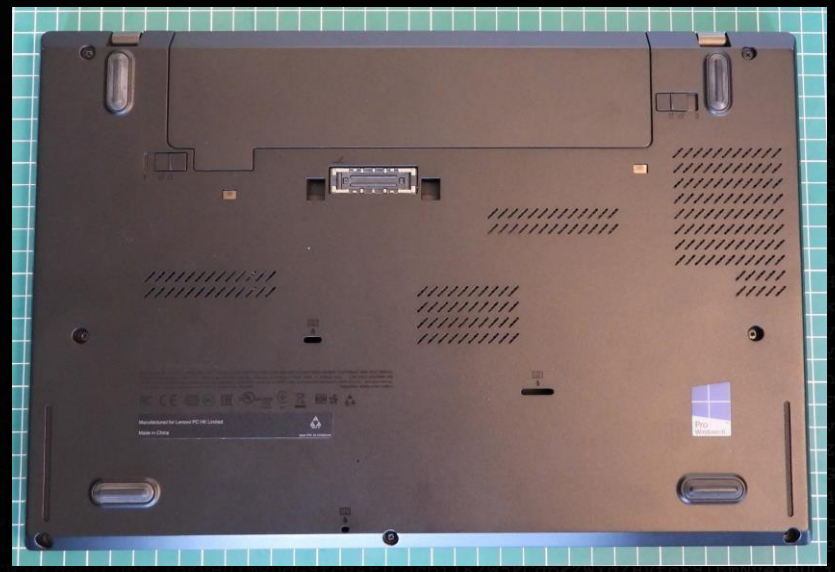
Notebook Disassembly

https://www.digitec.ch/de/s1/product/lenovo-thinkpad-x260-1250-intel-core-i7-6500u-8-gb-256-gb-ch-notebook-5928272

Notebook Disassembly

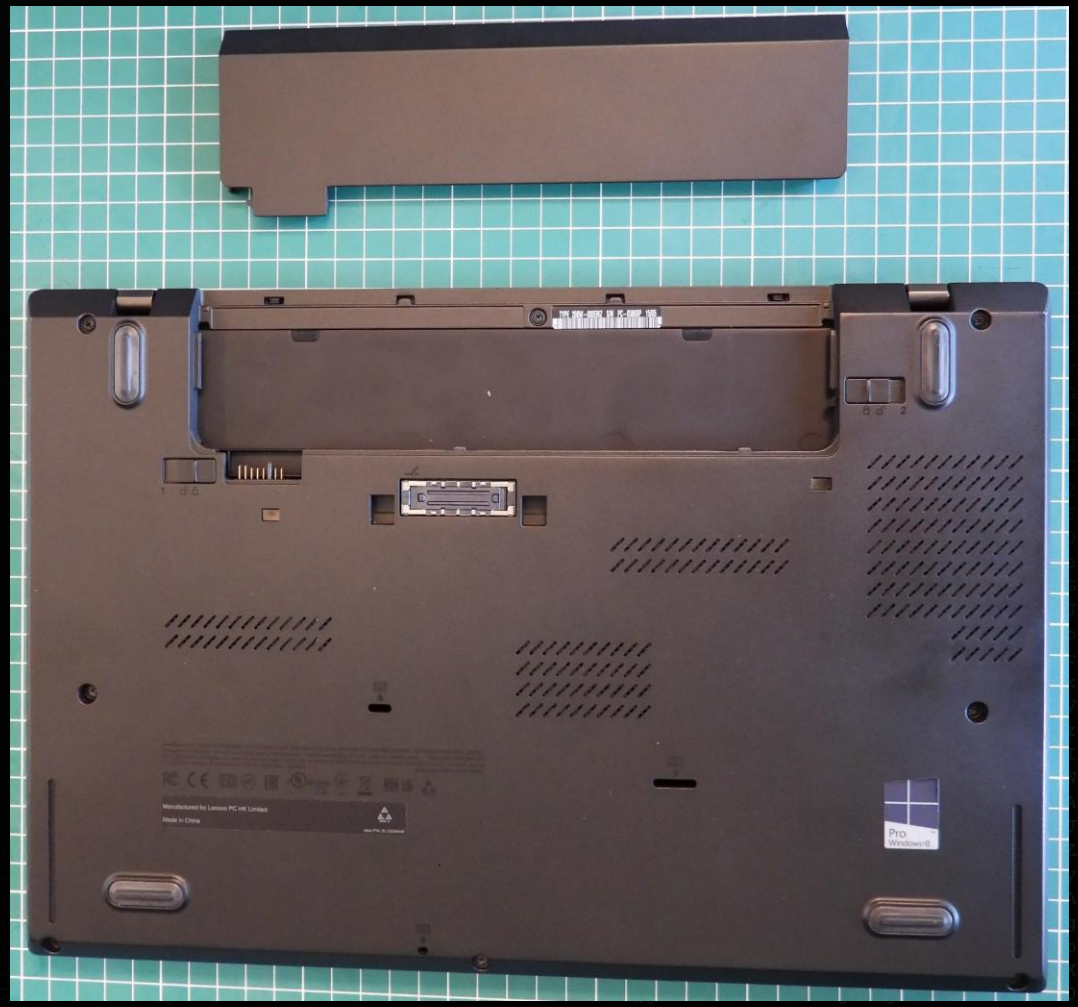
- Starting the Notebook (Functional Check)
- Shut down the notebook
- Start disassembling





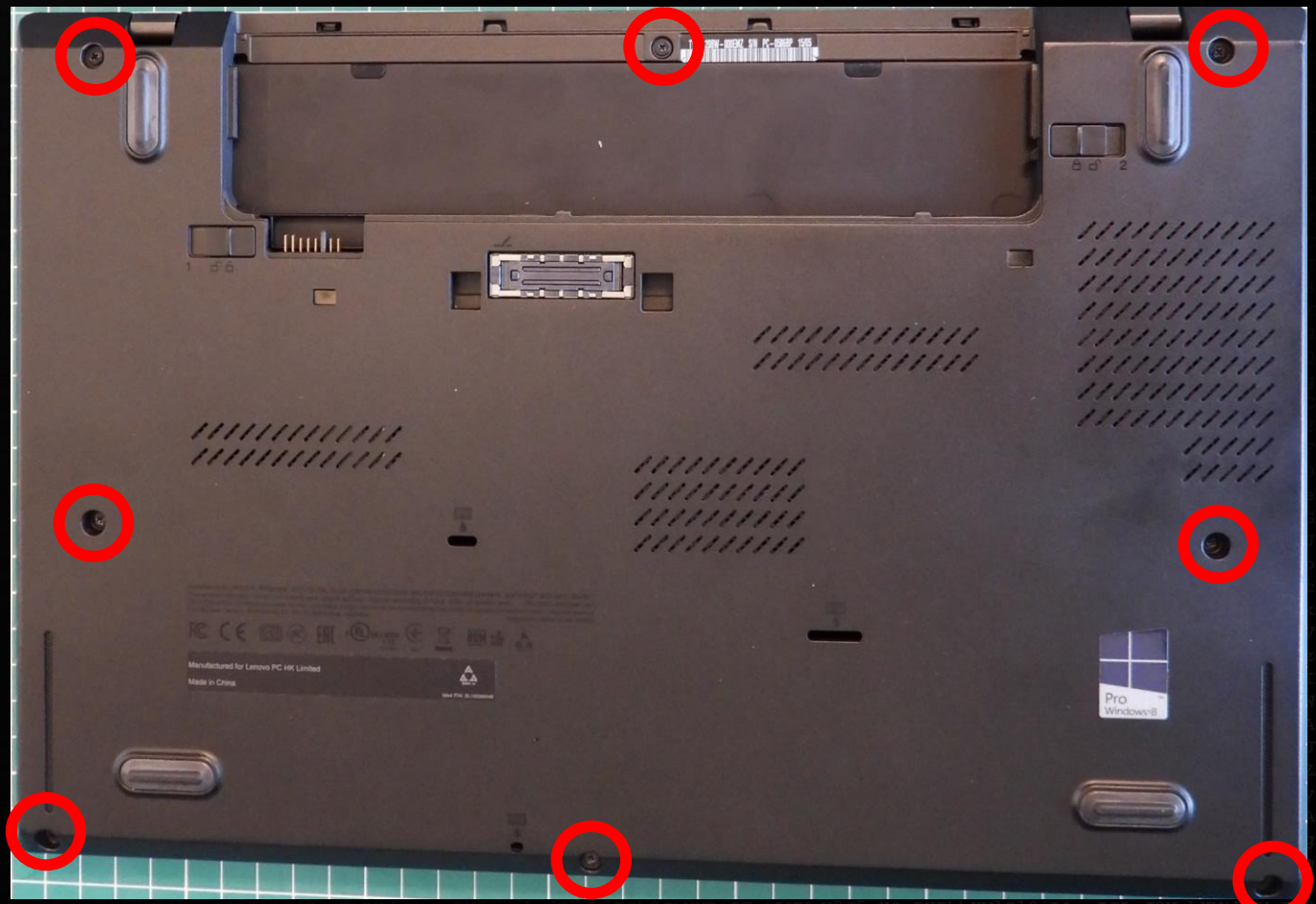
Notebook Disassembly

- Lenovo x260
- Remove the battery pack



Notebook Disassembly

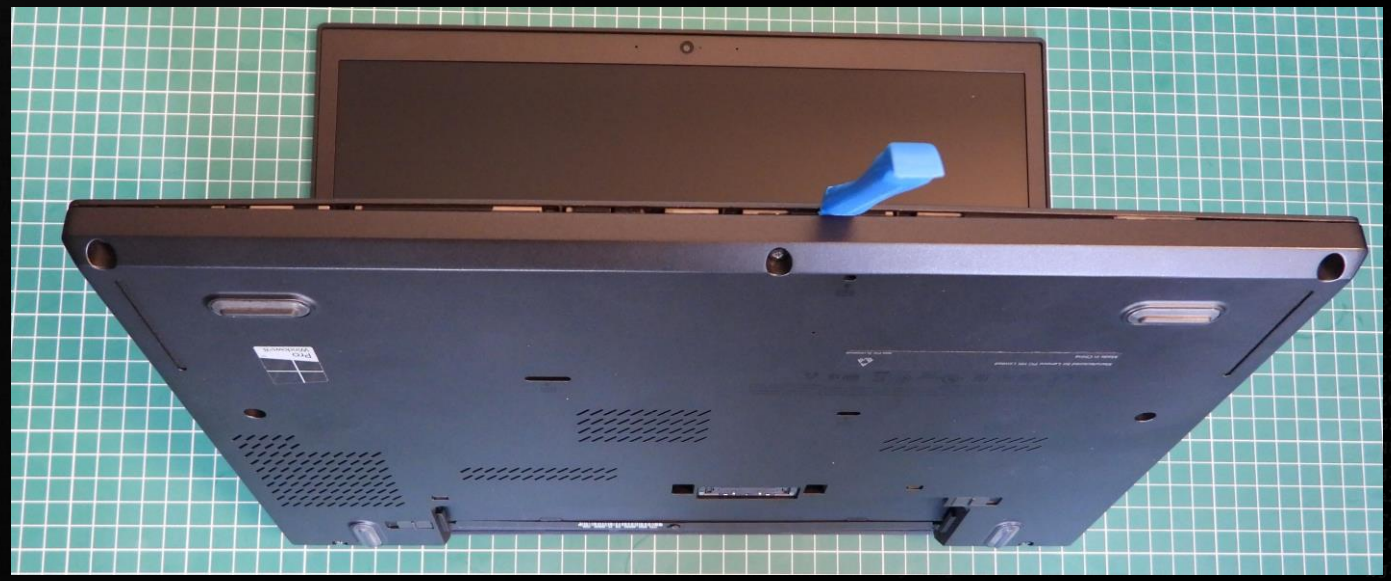
- Remove all screws



black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Notebook Disassembly

- Start with the opening in the middle
- Open the housing all around
- **Be careful, there may be some wires close to the edge**

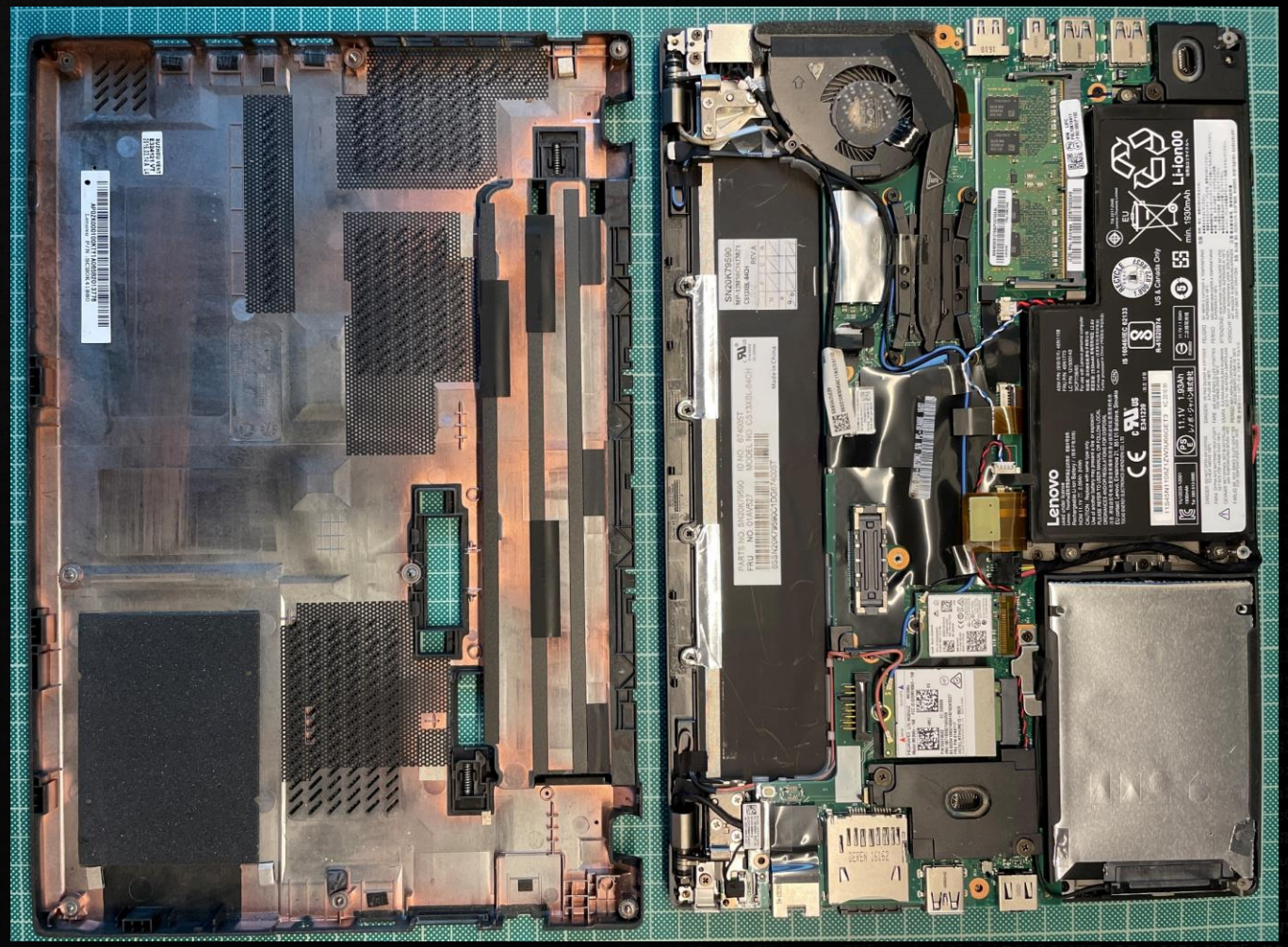


Notebook Disassembly

- Be careful, there may be some wires close to the edge

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Notebook Disassembly



black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Notebook Disassembly

- First overview the inside of your Lenovo x260

Tamper Protection

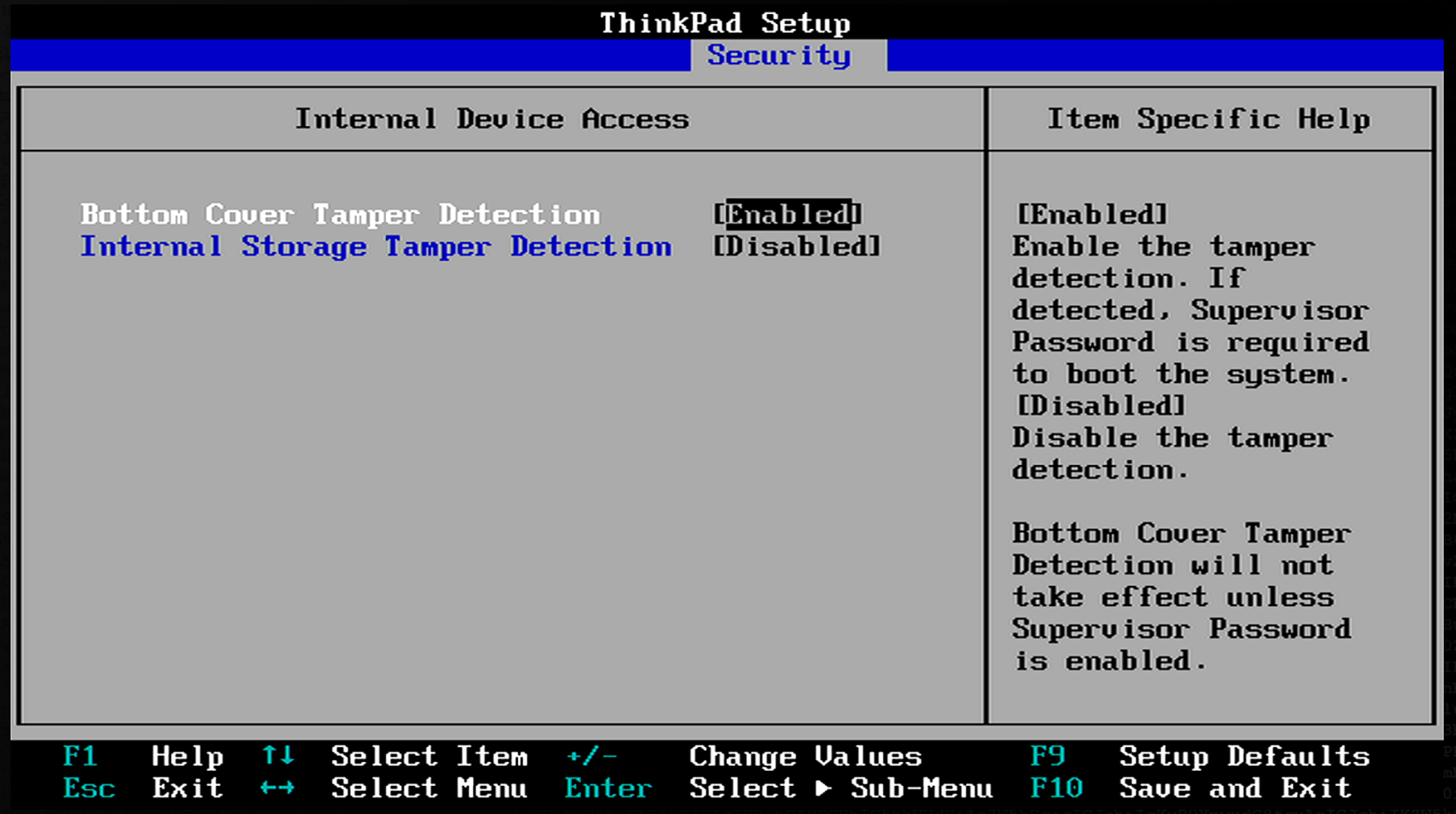
```
System Security - Bottom cover tamper detected

Press ESC to Continue
```

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Tamper Protection

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

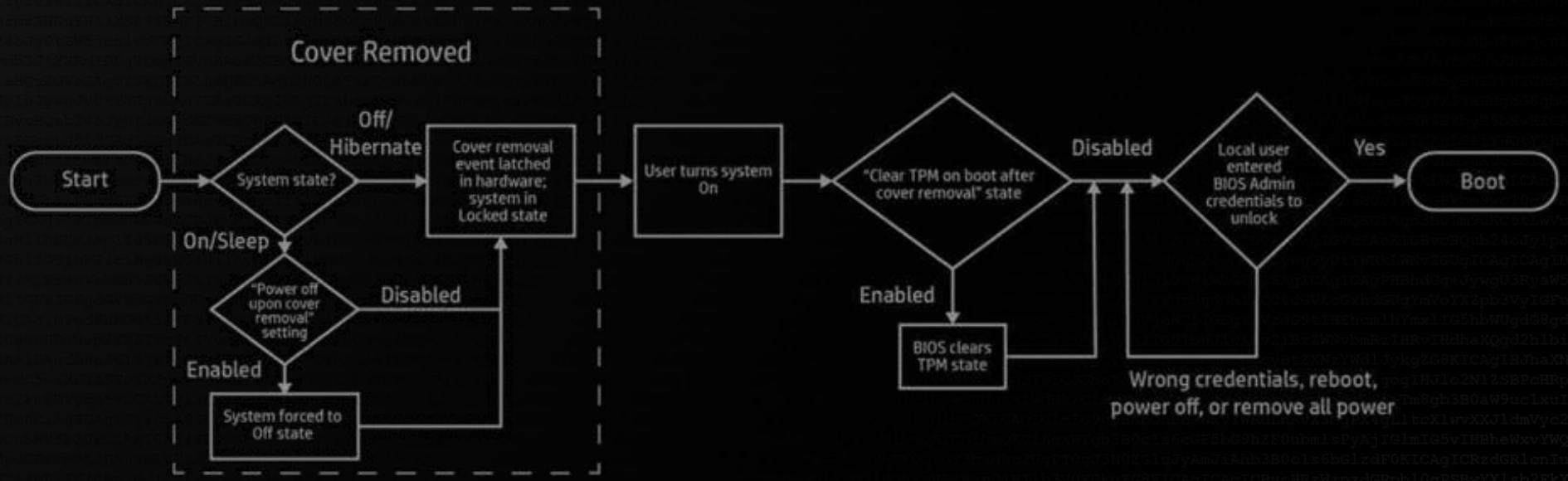
Tamper Protection



Tamper Protection

- HP TamperLock

HP WOLF SECURITY

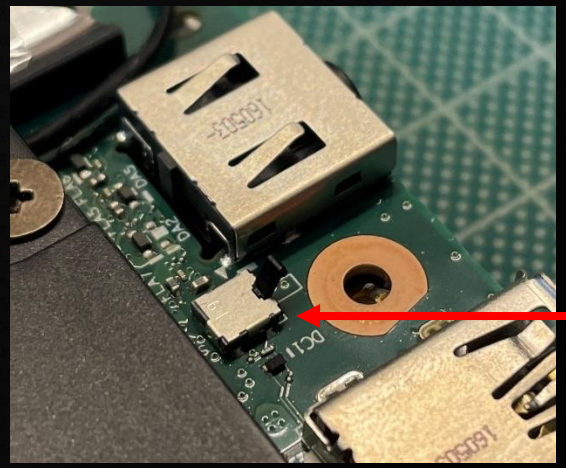


HP TamperLock User Guide http://h10032.www1.hp.com/ctg/Manual/c07055601.pdf

HP TamperLock White Paper https://h20195.www2.hp.com/v2/getpdf.aspx/4AA7-8167ENW.pdf

Tamper Protection

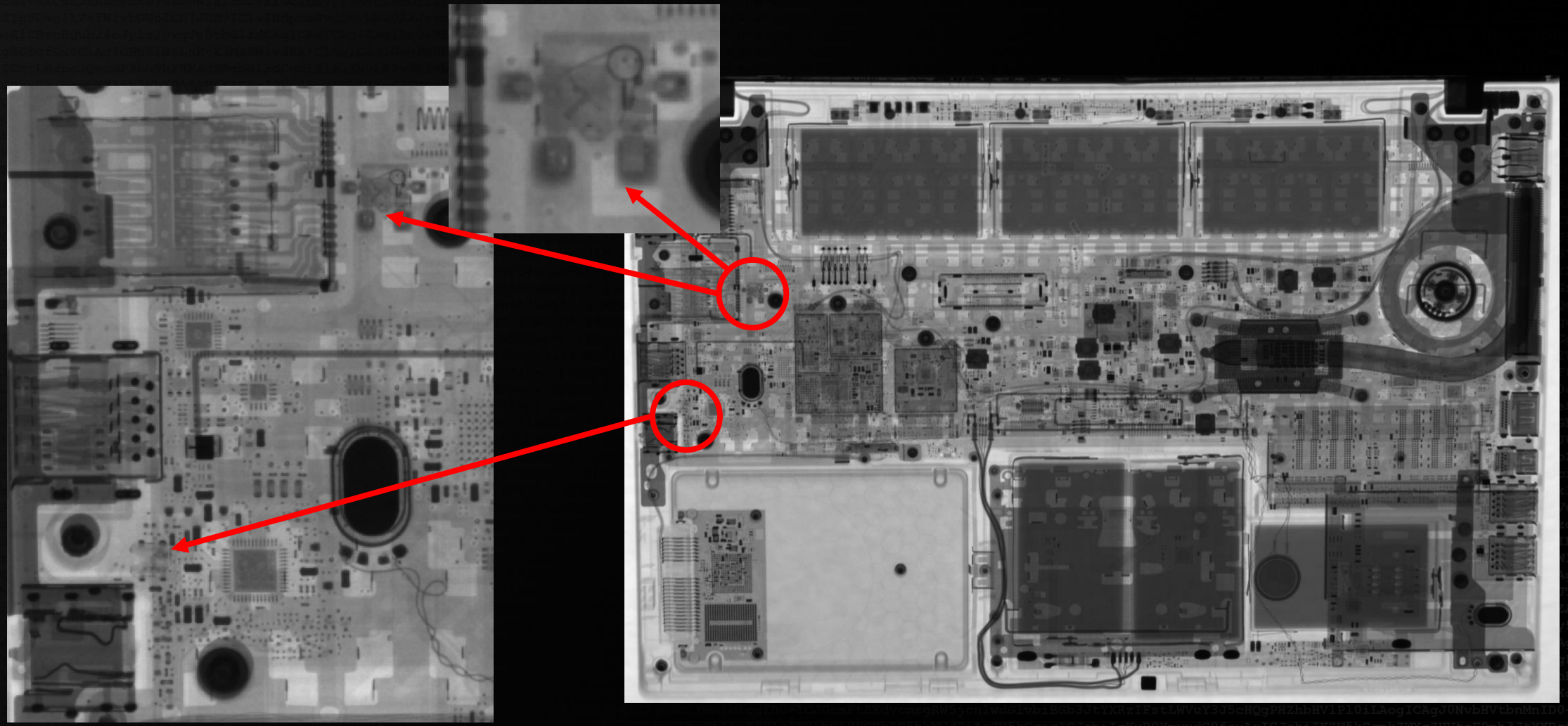
- Lenovo ThinkShield Built-in Platform Security (aka Tamper Switch)



ThinkShield

https://techtoday.lenovo.com/ch/de/solutions/large-enterprise/thinkshield

Tamper Protection – Lenovo x260



black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Tamper Protection Switch

- Different types of switches

switch type	normally open	normally closed
known vendor	Hewlett Packard (HP)	Lenovo
closed case	switch pressed; circuit closed	switch pressed; circuit open
opened case	switch released; circuit open	switch released; circuit closed
workaround (keep switch pressed)	bypass	remove switch

It's easier to keep a circuit closed than to prevent it from closing.

Tamper Protection Switch

- Defeating
  - Is it required to open the case completely? → Dremel your way!
  - Measure the switches on a test device: Are the switches normally open or normally close?
  - Drilling some holes in the case, to bypass the switches or unsolder the switches.

Expect the switches to be activated; once triggered, there might be no way back!

Tamper Protection Switch

Agenda Day 1

- Equipment Inspection
- Soldering Theory & Lab
- Tamper Protection Switches
  - Forensic Data Acquisition
  - Notebook Internals
  - Notebook Disassembly

Key Takeaways

- Ability to Solder
- Tamper Protection Switches
  - Basic Forensic Data Acquisition

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Forensic Data Acquisition

- Legal Authorization
- Chain of Custody
- Preparation
- Documentation
- Forensic Imaging
- Verification & Validation
- Storage & Preservation
- Reporting
- Forensic Boot Systems
- Hard Disk Inspection

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Legal Authorization

Forensic Data Acquisition

- Search Warrant
- Consent of the Owner

- Legal Procedures & Guidelines in case of company device

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Chain of Custody

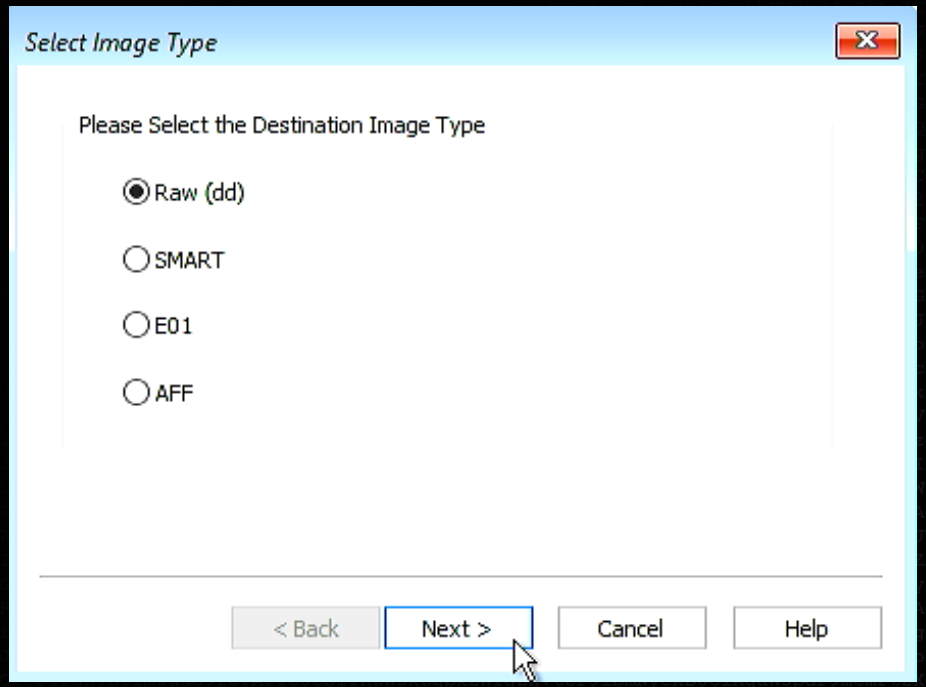
Forensic Data Acquisition

- Documentation of who has when custody (at all times)
- Tamper-evident documentation

Preparation

Forensic Data Acquisition

- Slightly bigger storage device than source device
- Write-blocker (software/hardware)
- Image Format
- Imaging Tools



Preparation

Forensic Data Acquisition

- Formats

Format	Description	Advantages	Disadvantages
E01 / EX01	Encase Evidence File Format	- Supports compression and encryption - Allows for segmented acquisition - Integrity checks / hashing integrated	- Proprietary format - Well reversed / ewfacquire - Not supported by all forensic tools
dd / raw	Raw Disk Image Format	- 1:1 copy of the disk/partition - Can be mounted, analyzed and carved without additional tools	- No built-in compression or encryption - Integrity not guaranteed
AD1	AccessData Forensic Image Format	- Captures logical files and directories - Allows for selective acquisition - Supports compression and encryption - Allows for segmented acquisition	- Proprietary format - Requires commercial software to create and analyze - Not widely supported by other forensic tools
L01	Logical Evidence File Format	- Captures logical files and directories - Allows for selective acquisition	- Proprietary format - No Image Hash, only hashes for files inside - May require additional processing for analysis
AFF	Advanced Forensic Format	- Supports compression and encryption - Allows for segmented acquisition - Integrity checks / hashing	- Not widely supported by other forensic tools

Preparation

Forensic Data Acquisition

- Tools

dd

dc3dd

Cellebrite UFED

Guymager

X-Ways

MAGNET FORENSICS

EnCase® Forensic
by Guidance Software

PALADIN

opentext™ | EnCase™

OXYGEN FORENSICS

Windows Forensic Environment

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Documentation

Forensic Data Acquisition

- Document all your steps
- “Personal” notes – not part of the records
- Essential for writing the report

Forensic Imaging

Forensic Data Acquisition

Verification & Validation

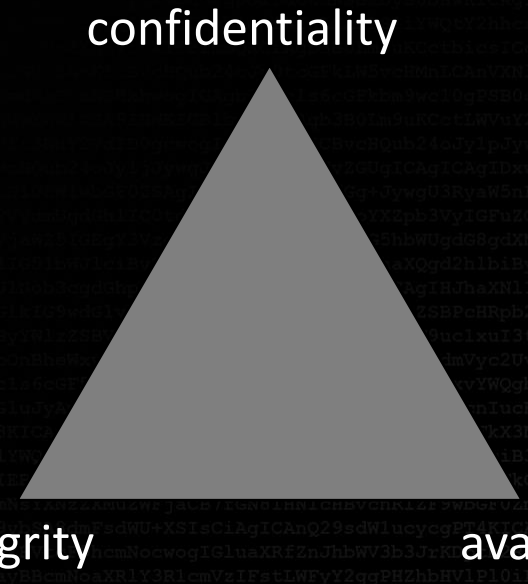
Forensic Data Acquisition

- Let the image verification process finish
- Do manual validation if you did the right thing
- Compare hashes also when copying acquired images

Storage & Preservation

Forensic Data Acquisition

- Prevent unauthorized access, tampering or loss
- Redundancy (Geo-redundancy?)



Reporting

Forensic Data Acquisition

- Convert your personal notes to a proper report
- Documents the entire data acquisition process
- All the steps, tools and results

Your report is not just a document,

it’s the foundation of informed decision-making.

Forensic Boot Systems

Forensic Data Acquisition

- No adapters needed
- Quick and convenient
- Only software write-blocker

PALADIN

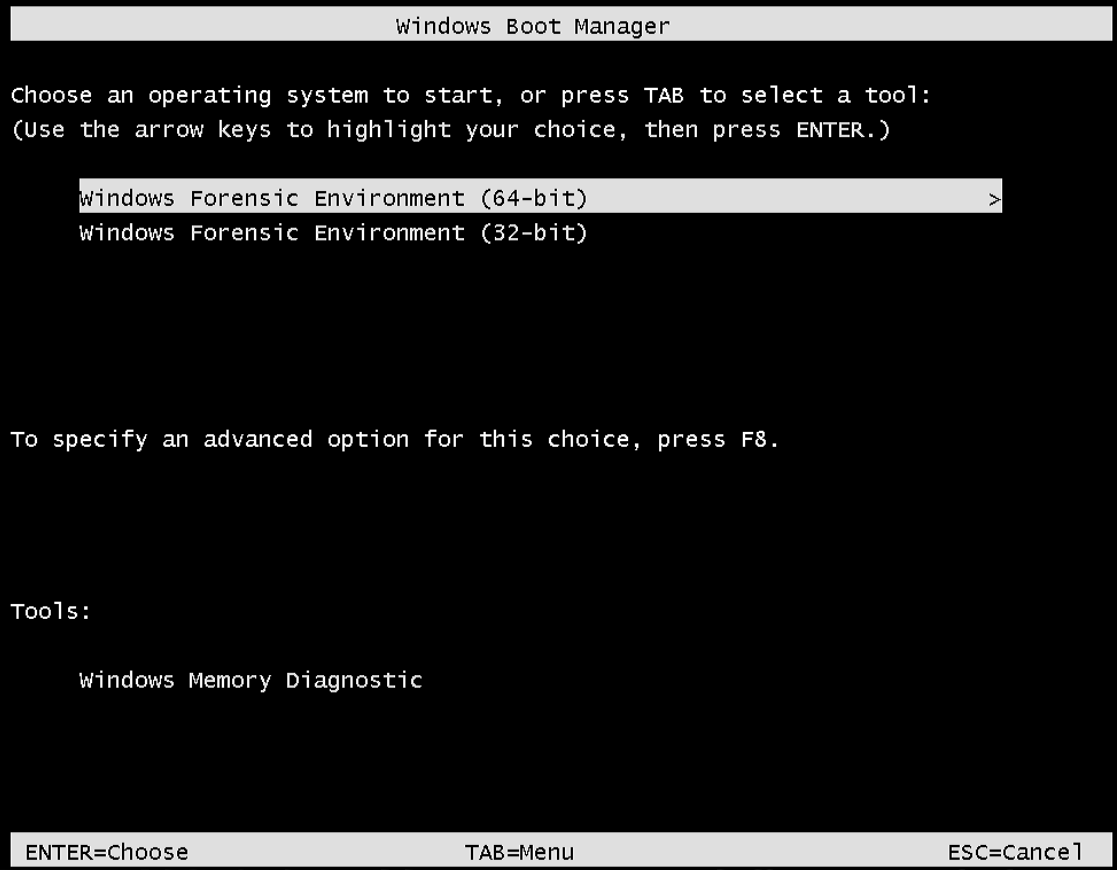
Windows Forensic Environment

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Forensic Boot Systems

Forensic Data Acquisition

- Requirements for Target
  - Boot from external device must be possible
  - Or adjustable (no bios password set)
  - Compatible Boot Options enabled



black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Forensic Boot Systems

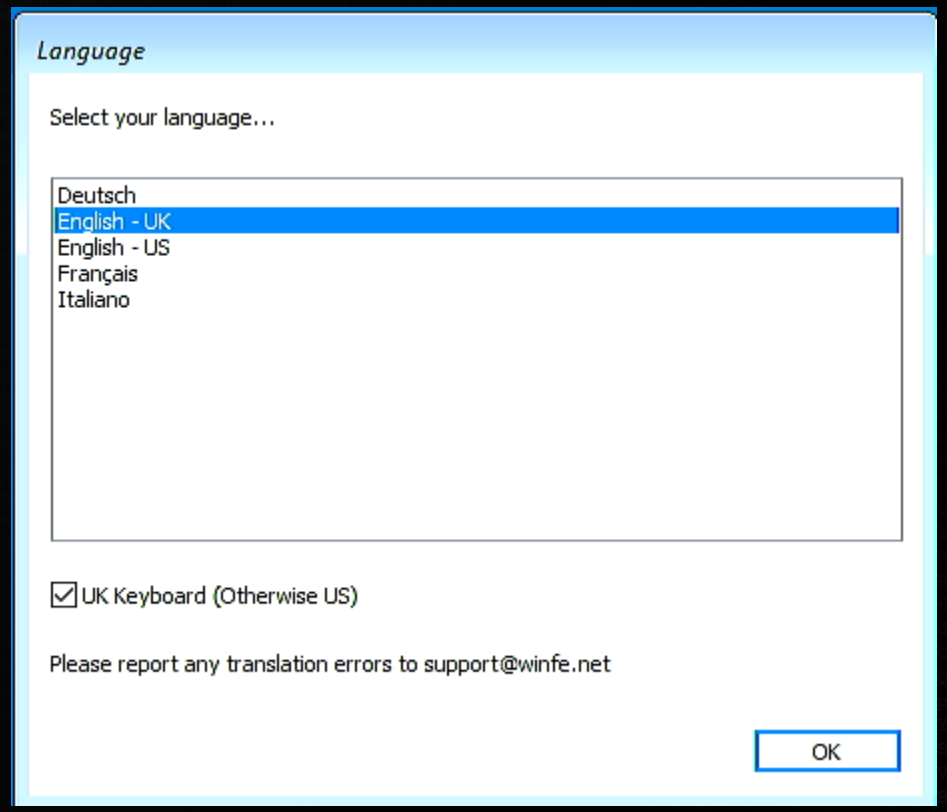
Forensic Data Acquisition

- UEFI (Unified Extensible Firmware Interface)
  - support for larger disk sizes
  - faster boot times
  - Secure Boot
  - graphical user interface (GUI)
- BIOS (Basic Input/Output System; Legacy)
  - traditional firmware interface
  - text-based interface
- CSM (Compatibility Support Module)
  - Enables BIOS-based boot loaders in UEFI environment

Do **NOT** alter under any circumstances!

Windows Forensic Environment

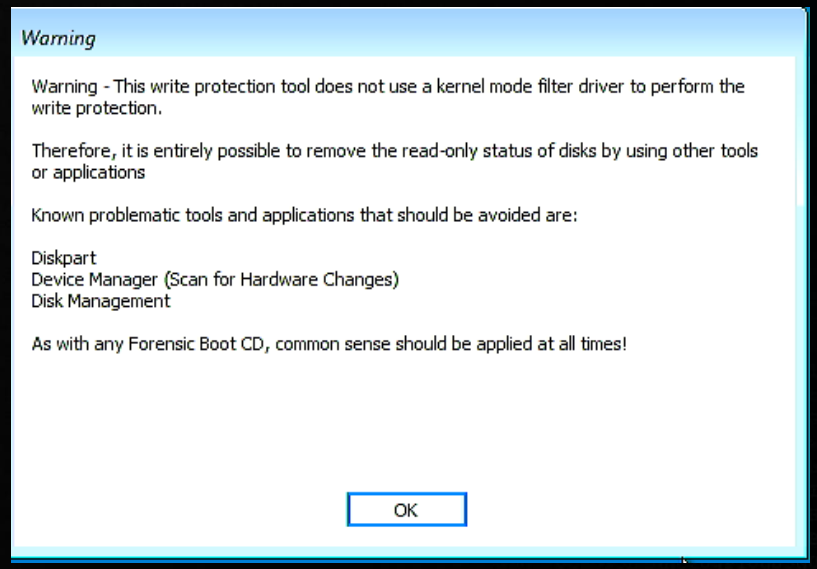
Forensic Data Acquisition



black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

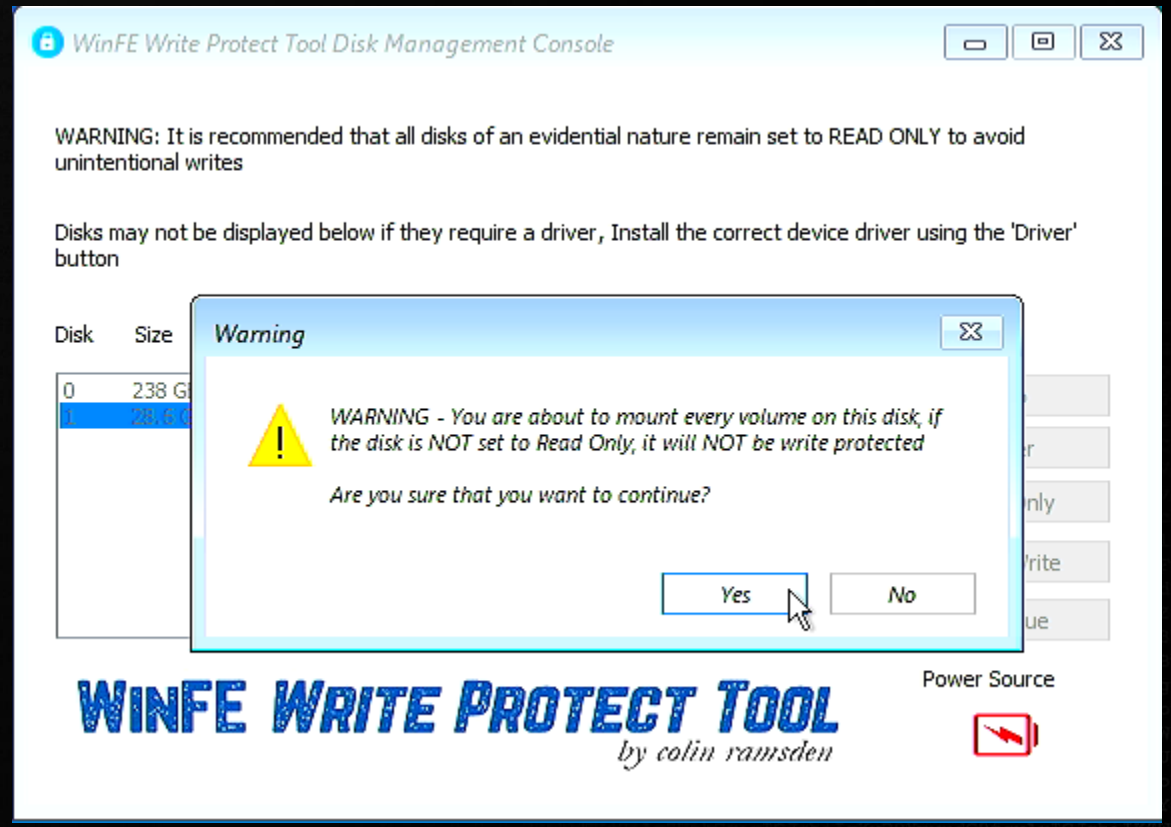
Windows Forensic Environment

Forensic Data Acquisition



Windows Forensic Environment

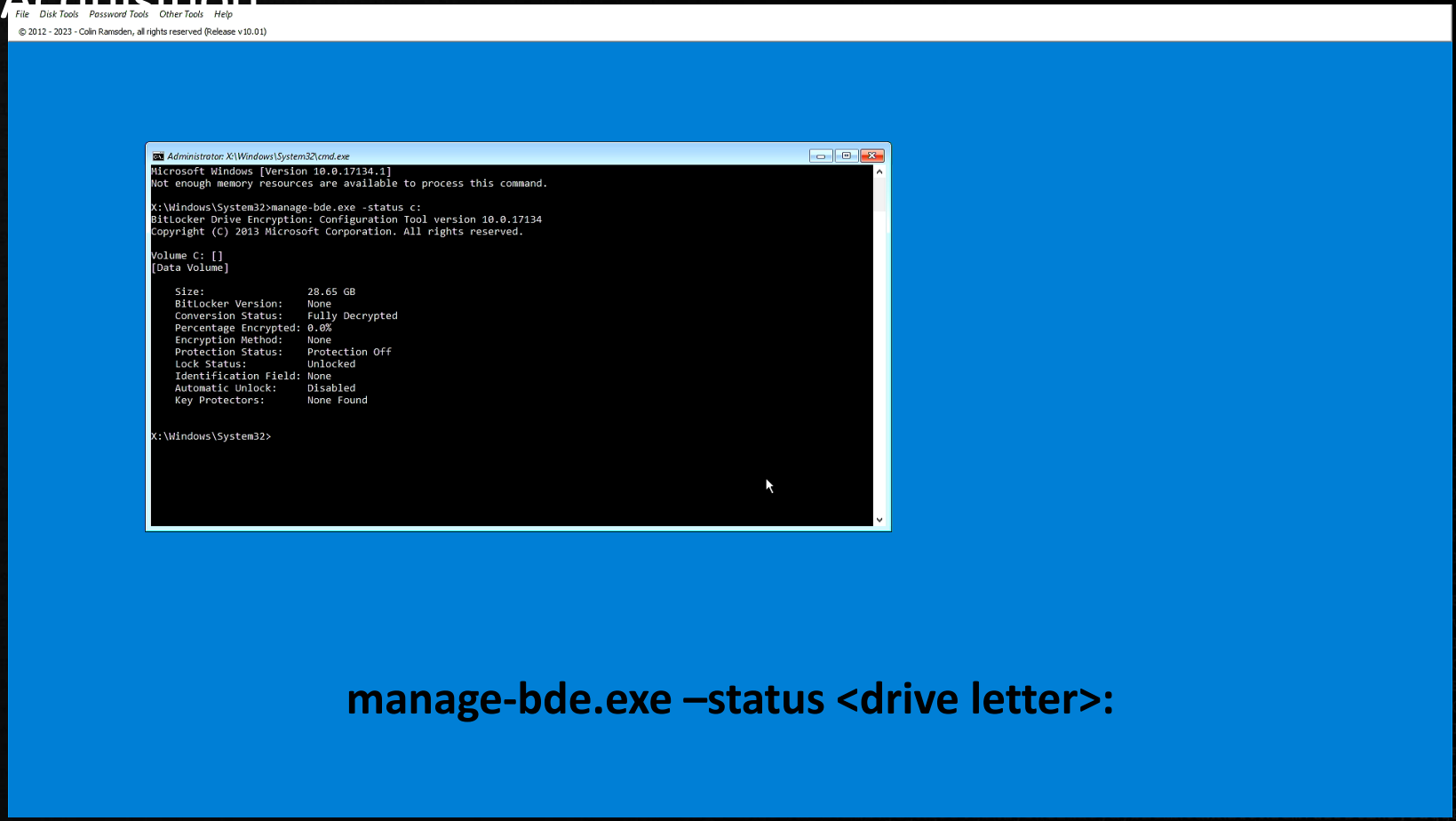
Forensic Data Acquisition



black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Windows Forensic Environment

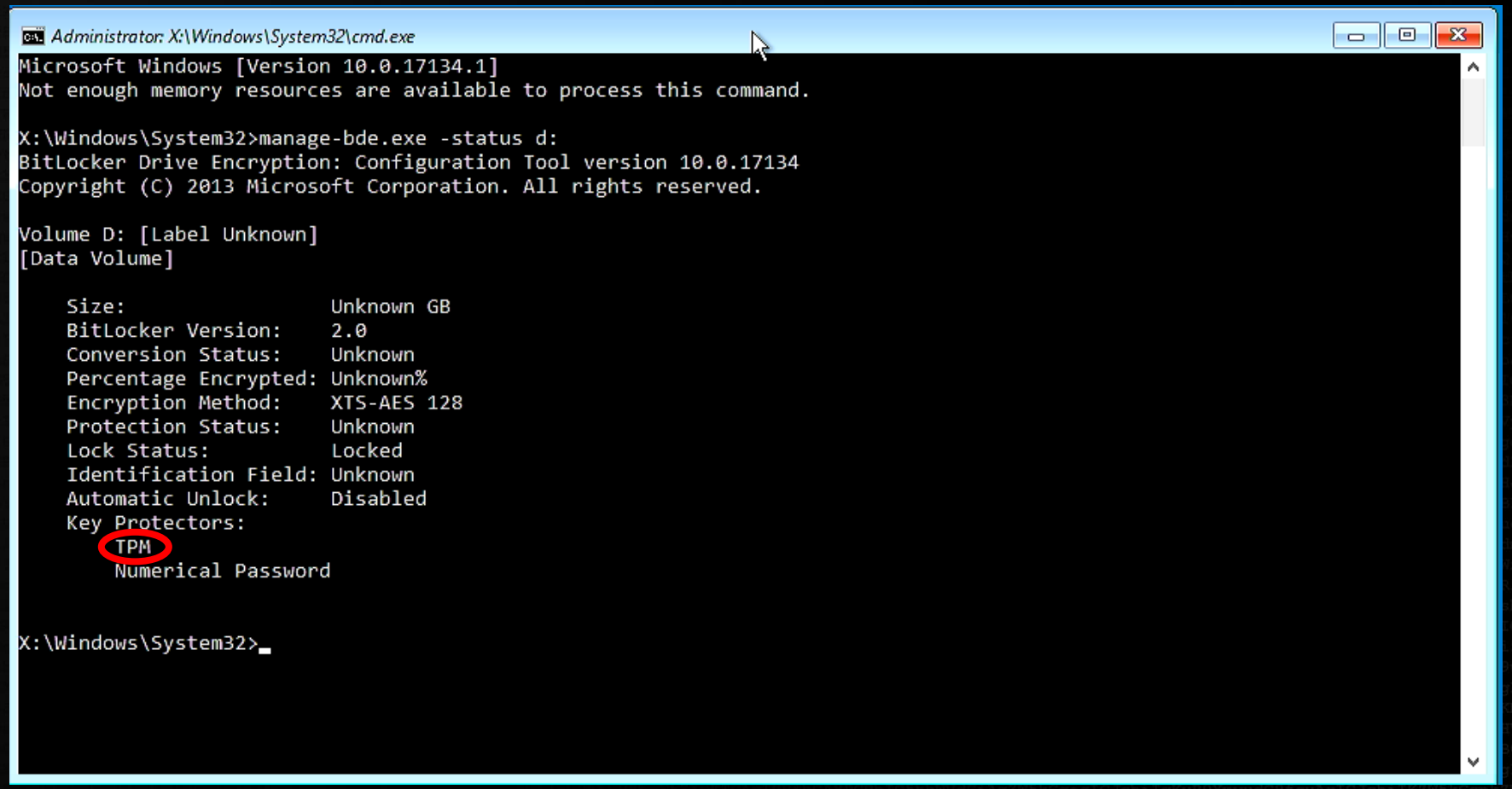
Forensic Data Acquisition



manage-bde.exe –status <drive letter>:

Windows Forensic Environment

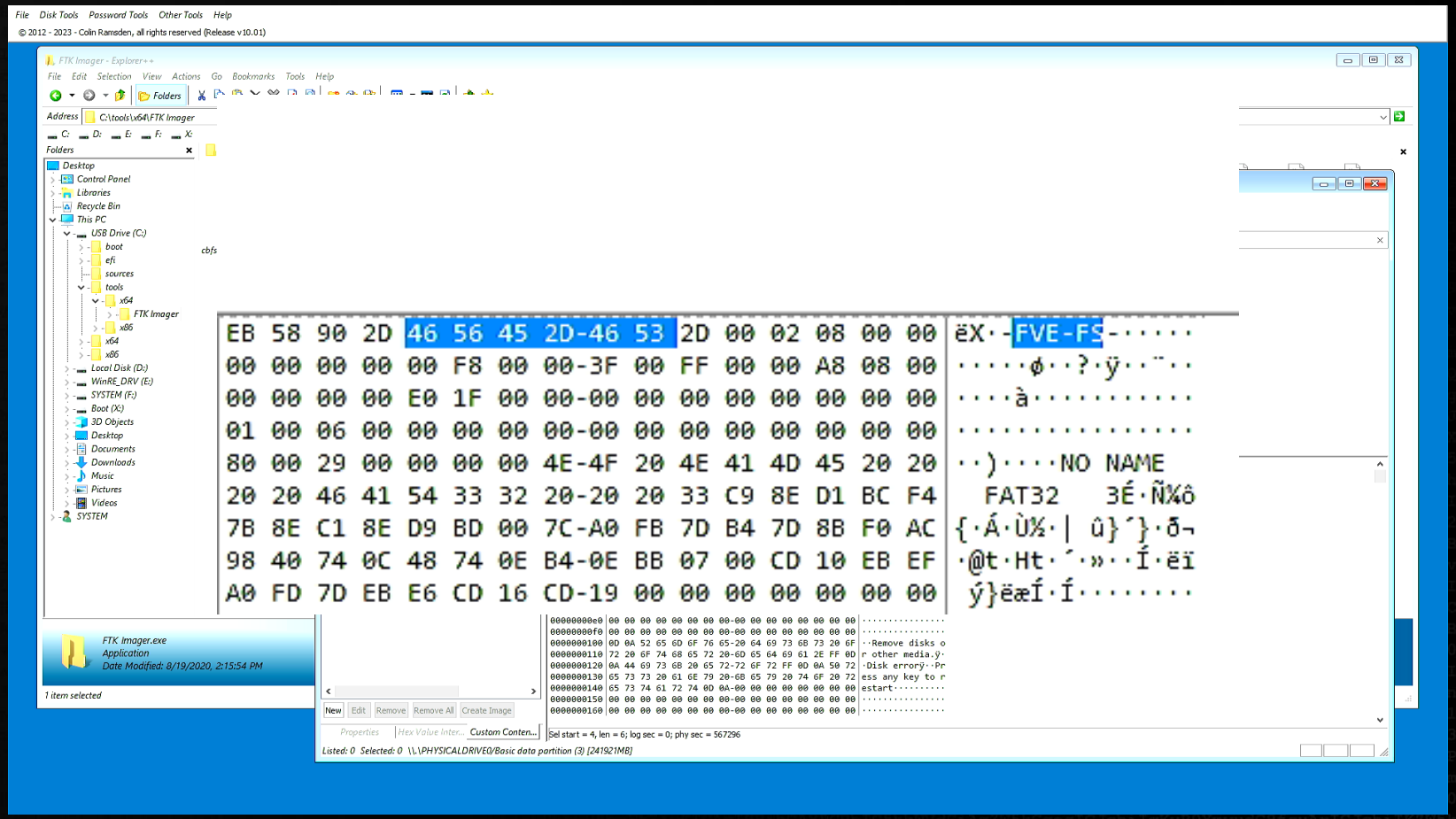
Forensic Data Acquisition



black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

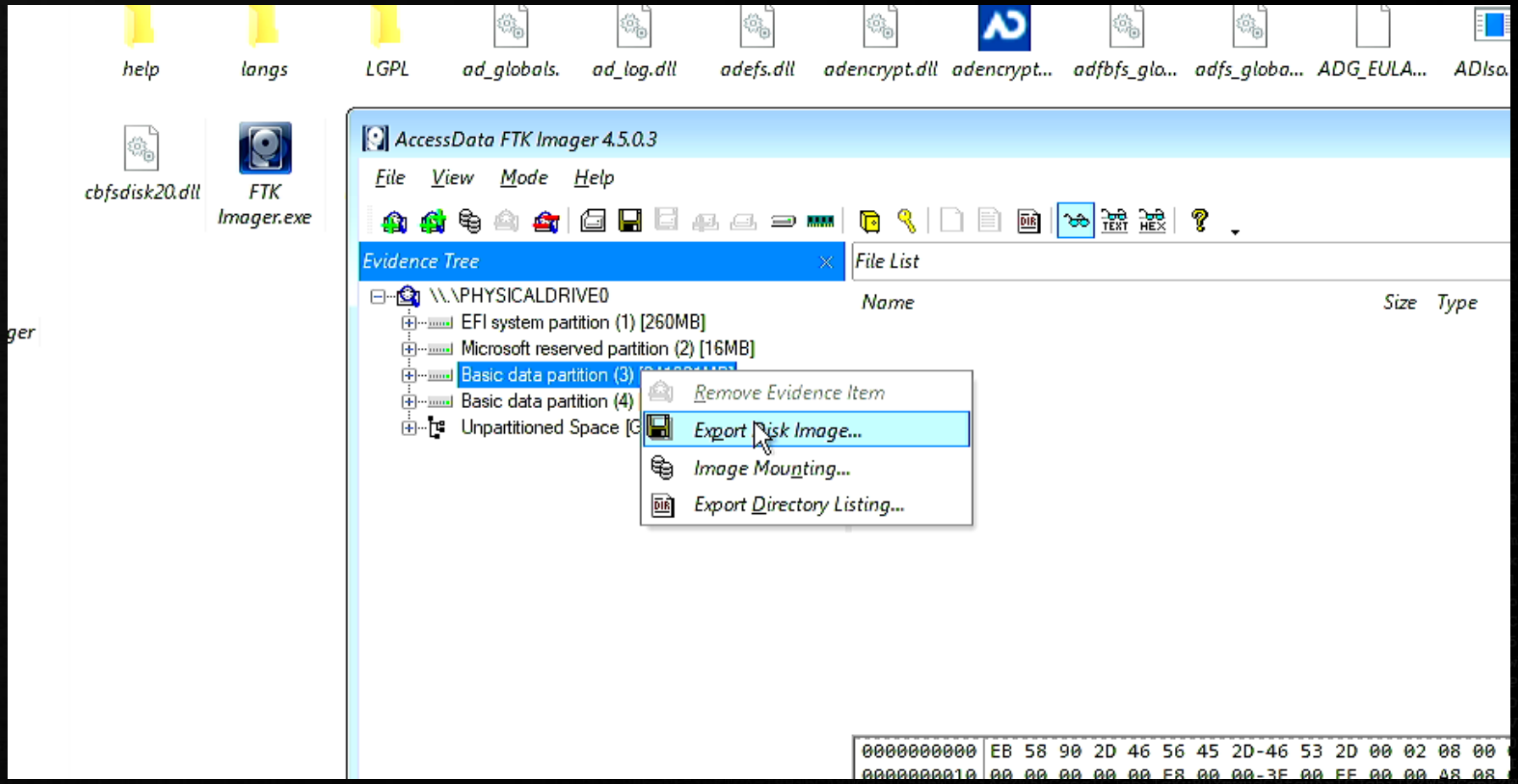
Windows Forensic Environment

Forensic Data Acquisition



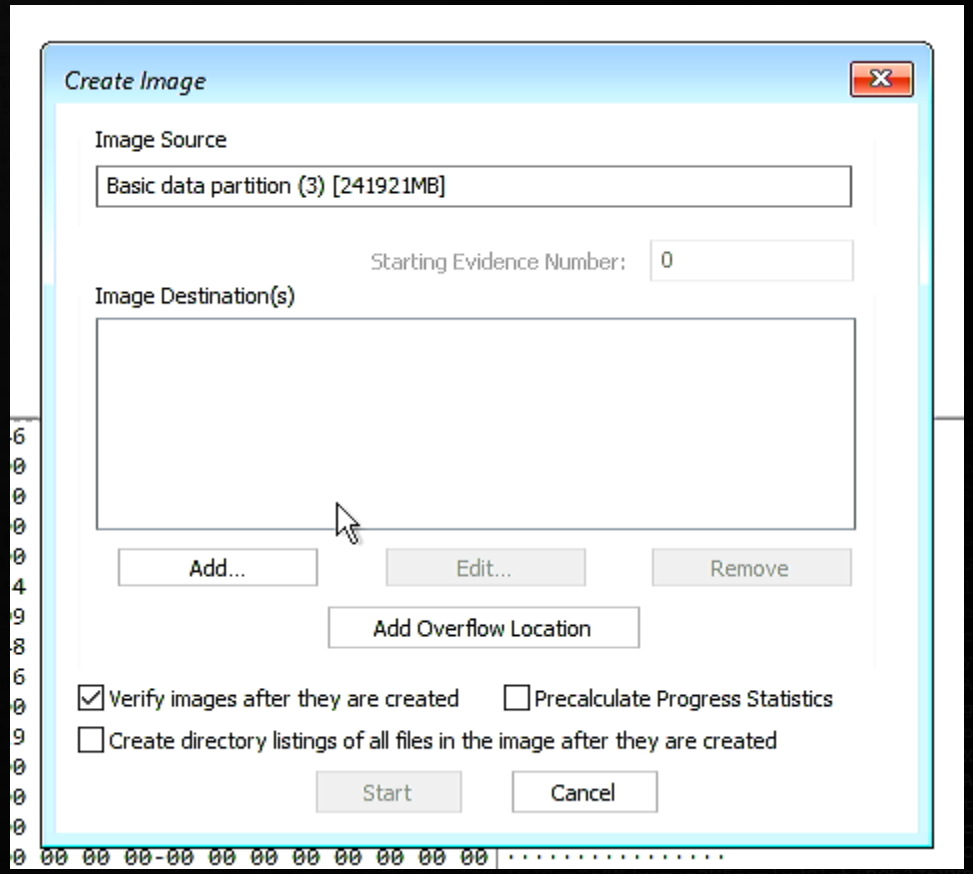
Windows Forensic Environment

Forensic Data Acquisition



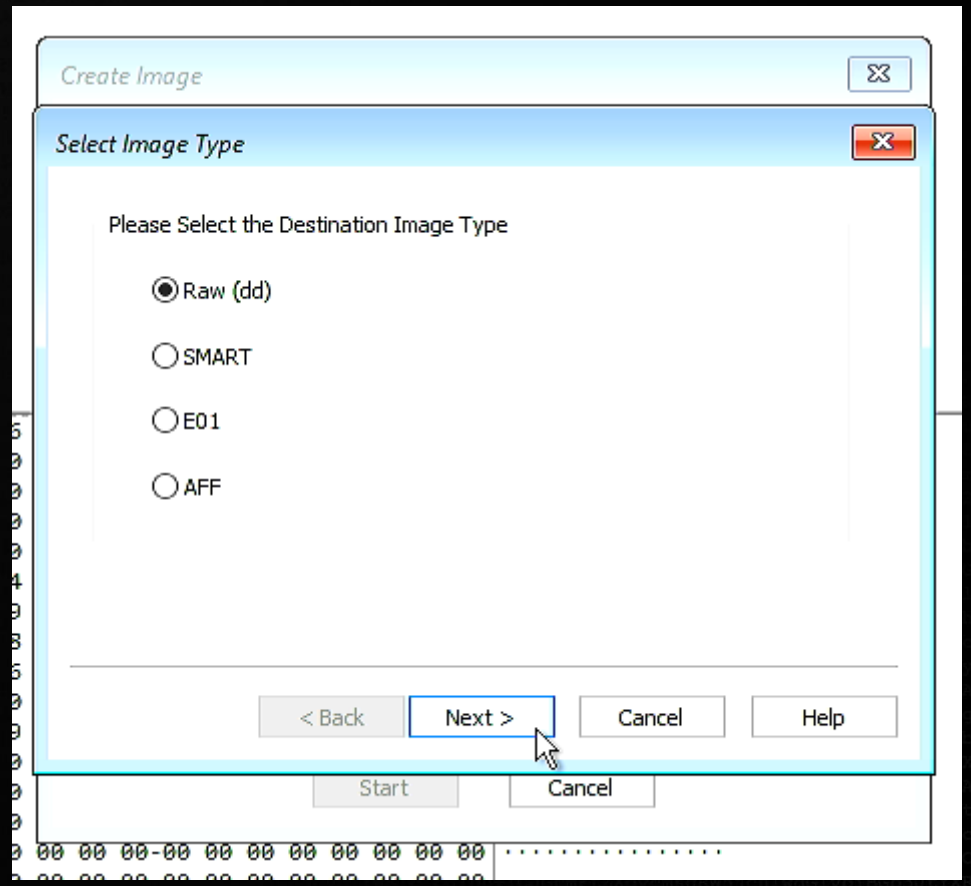
Windows Forensic Environment

Forensic Data Acquisition



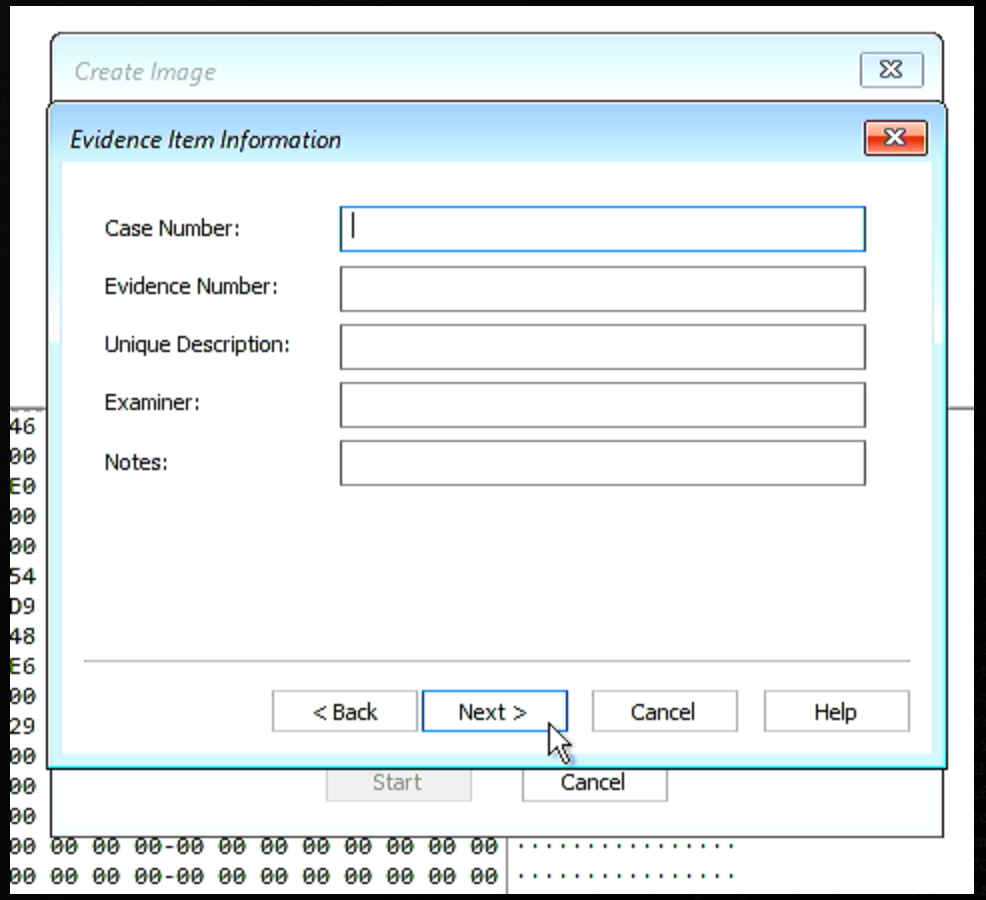
Windows Forensic Environment

Forensic Data Acquisition



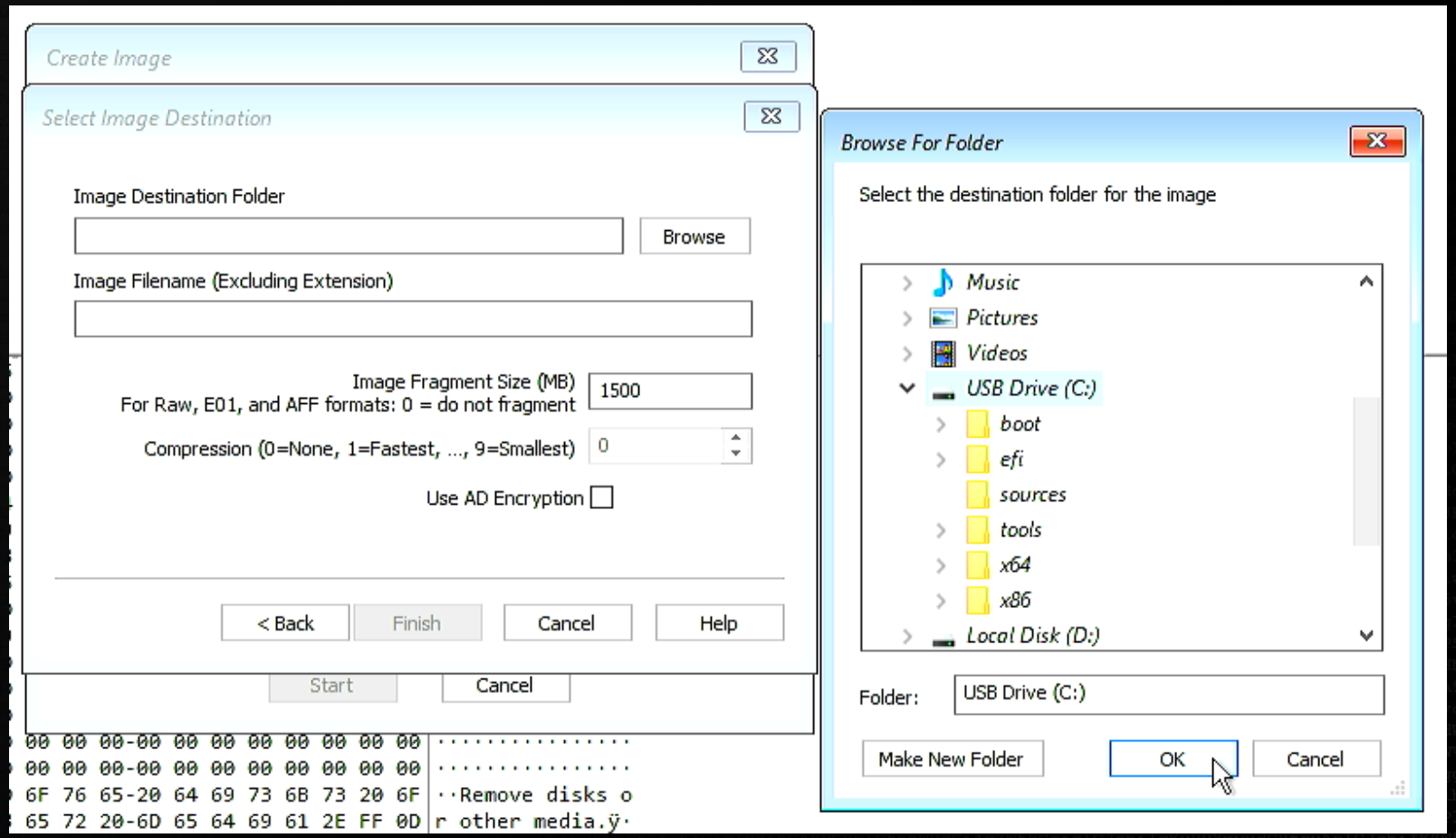
Windows Forensic Environment

Forensic Data Acquisition



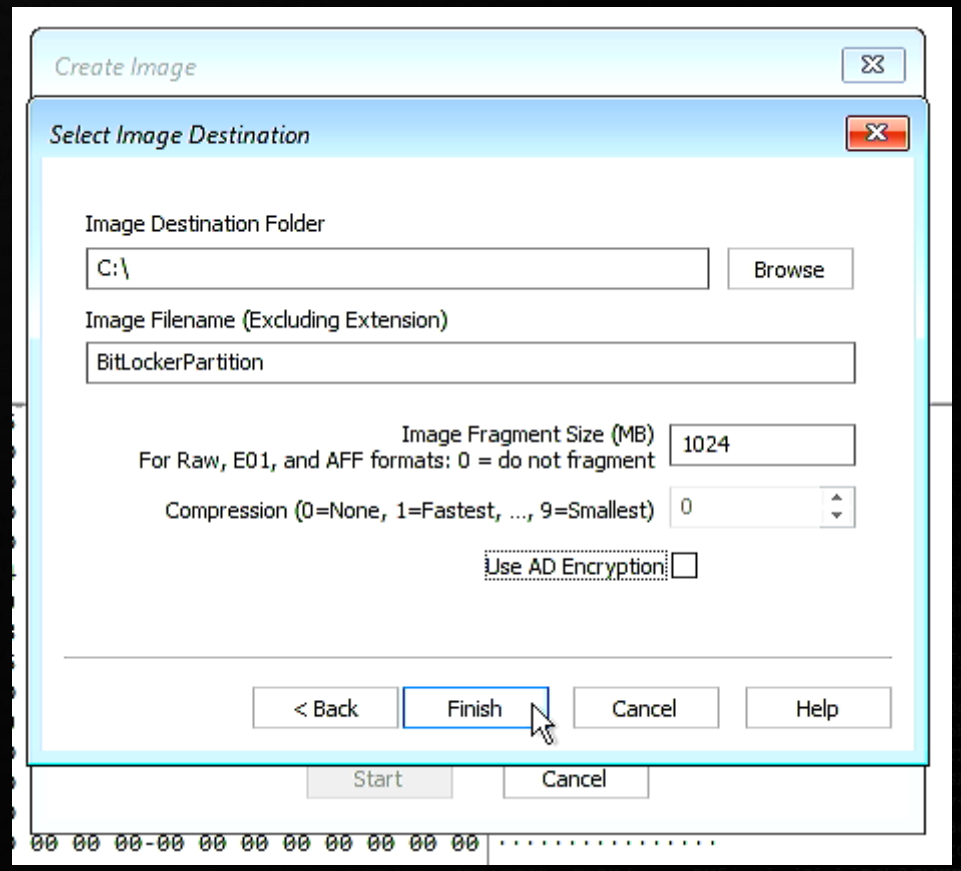
Windows Forensic Environment

Forensic Data Acquisition



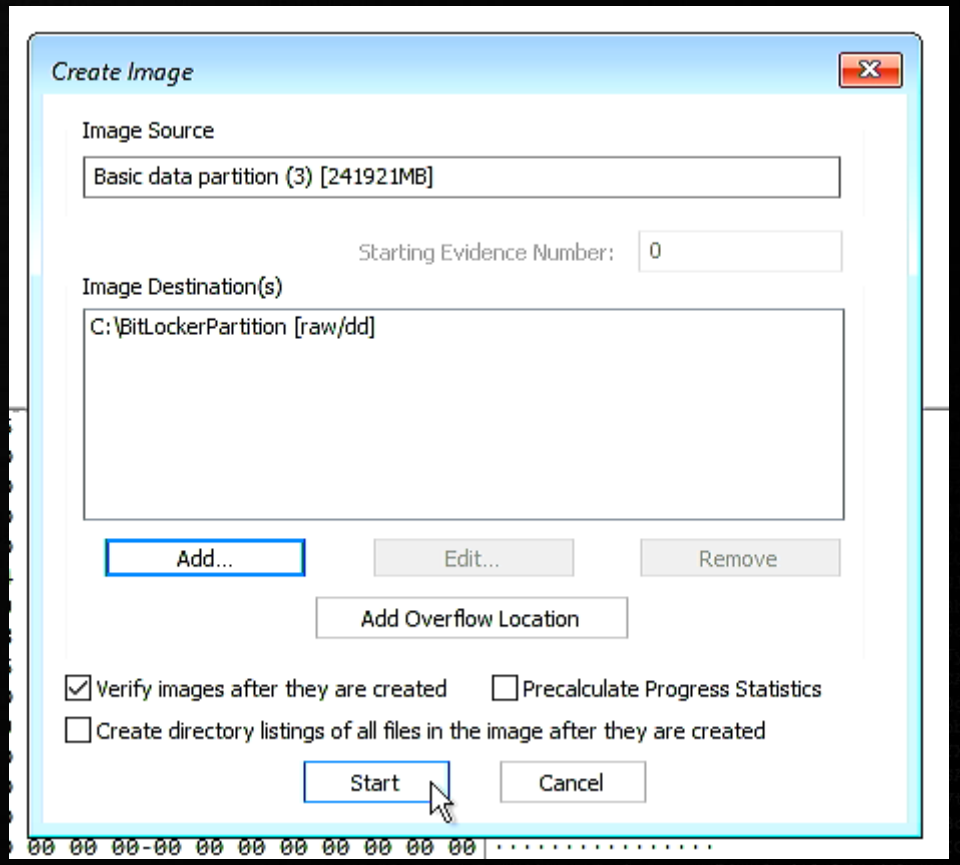
Windows Forensic Environment

Forensic Data Acquisition



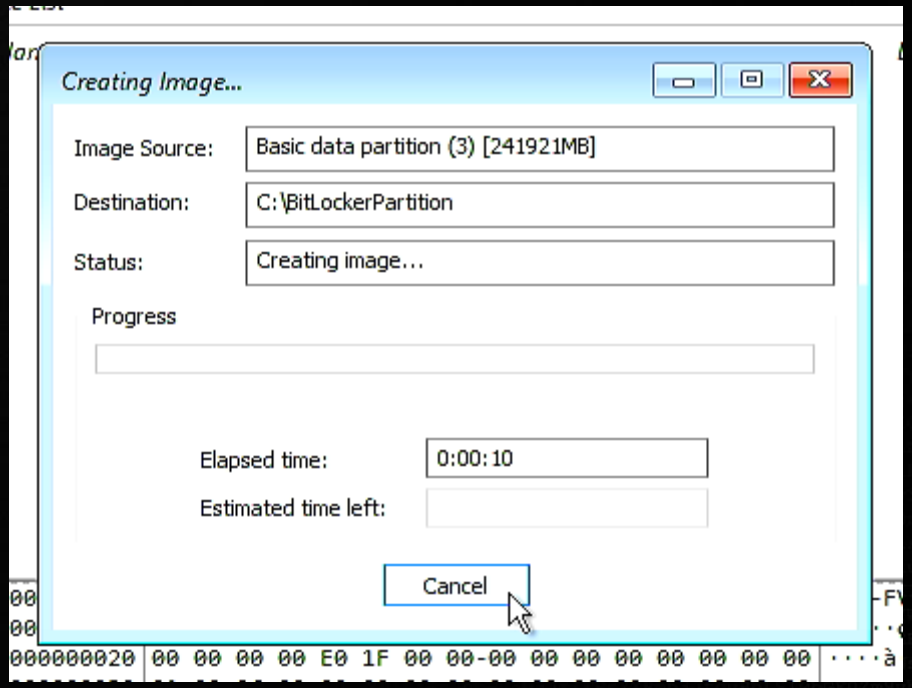
Windows Forensic Environment

Forensic Data Acquisition



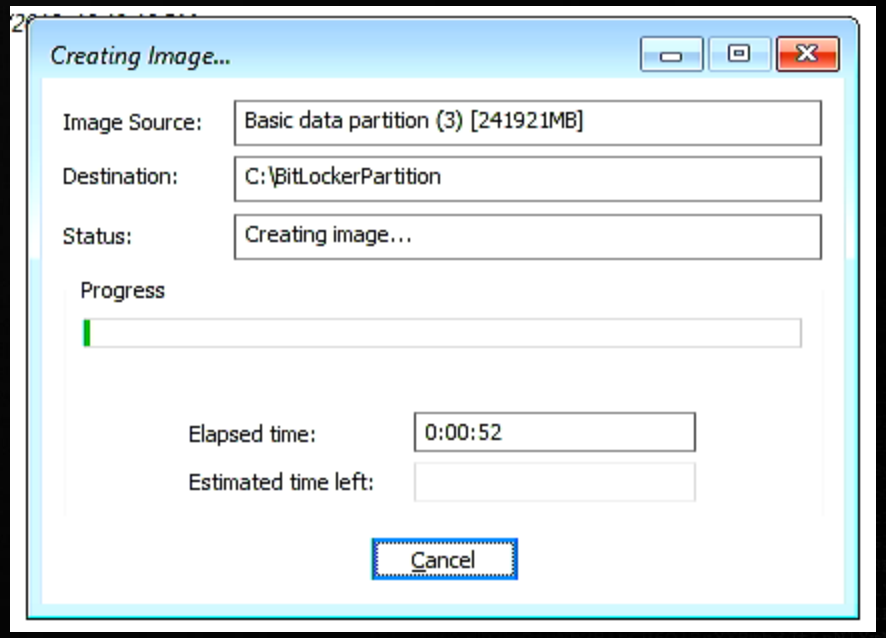
Windows Forensic Environment

Forensic Data Acquisition



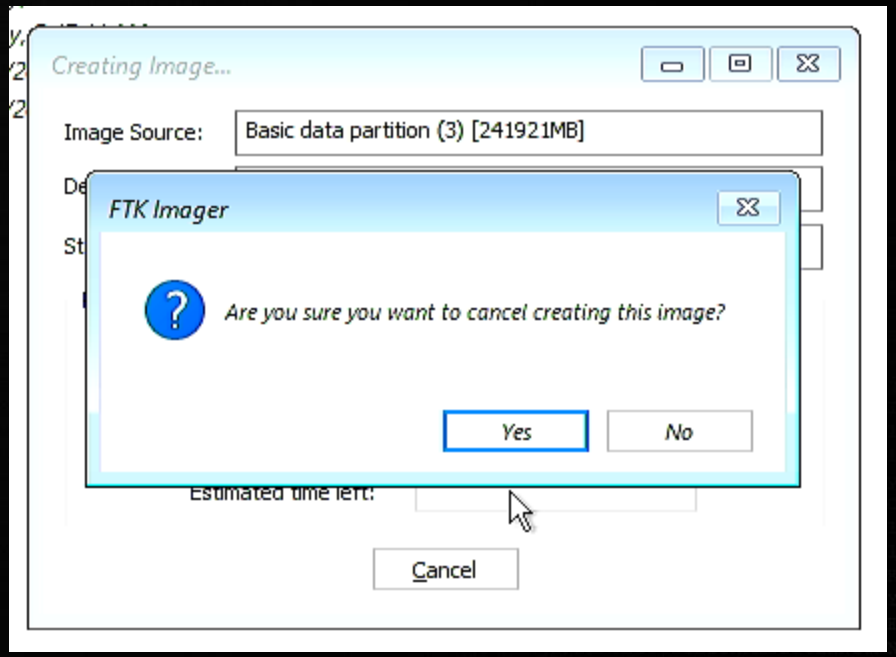
Windows Forensic Environment

Forensic Data Acquisition



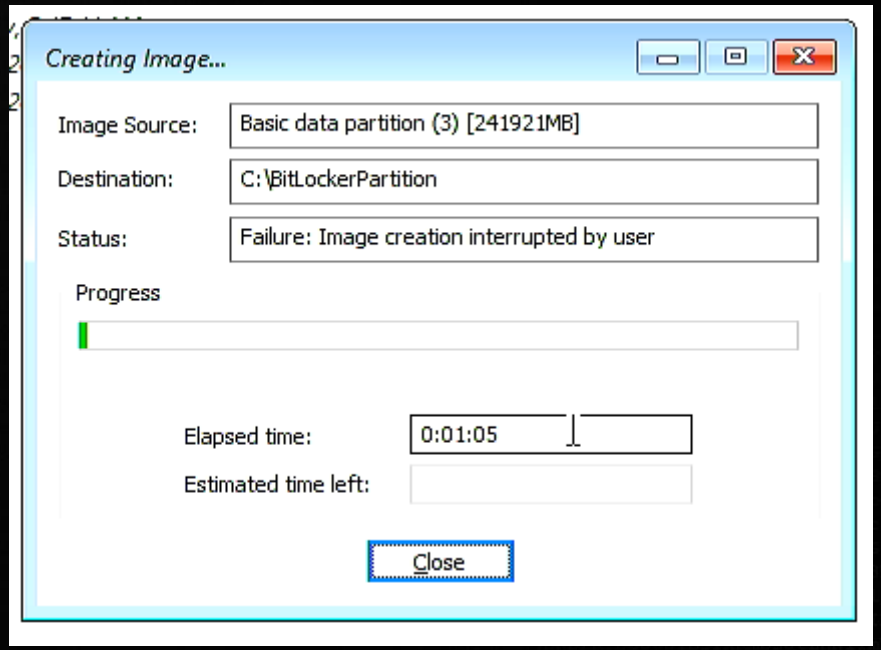
Windows Forensic Environment

Forensic Data Acquisition



Windows Forensic Environment

Forensic Data Acquisition



Hard Disk Inspection

Forensic Data Acquisition

- Task:
  - Boot WinFE
  - Check the BitLocker partition’s protectors using manage-bde.exe

  - Create a raw image of the first ~1 GB of the BitLocker protected partition (dd)
  - Analyze the created BitLocker header with dislocker-metadata in vm
  - Compare the outputs – what do you observe?

Hard Disk Inspection

Forensic Data Acquisition

- Launch the Ubuntu VM from your USB or install dislocker natively:
  - sudo apt update
  - sudo apt install dislocker

  - dislocker-metadata –V <path-to-your-BitLocker-header.dd>

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Hard Disk Inspection

Forensic Data Acquisition

```
Sun Apr 16 22:08:12 2023 [INFO] 0x00000020 ee 3c a8 b4 82 c4 7c ed-68 97 61
Sun Apr 16 22:08:12 2023 [INFO] ========================================
Sun Apr 16 22:08:12 2023 [INFO]
Sun Apr 16 22:08:12 2023 [INFO] =======[ Datum n°8 information ]===
Sun Apr 16 22:08:12 2023 [INFO] Total datum size: 0x0064 (100) byte
Sun Apr 16 22:08:12 2023 [INFO] Datum entry type: 15
Sun Apr 16 22:08:12 2023 [INFO] Datum value type: 15
Sun Apr 16 22:08:12 2023 [INFO]     `--> VIRTUALIZATION INFO -- Tota
Sun Apr 16 22:08:12 2023 [INFO] Status: 0x1
Sun Apr 16 22:08:12 2023 [INFO] NTFS boot sectors address:  0xa610(
Sun Apr 16 22:08:12 2023 [INFO] Number of backuped bytes: 0x2000 (8
Sun Apr 16 22:08:12 2023 [INFO] Unknown:
Sun Apr 16 22:08:12 2023 [INFO] 0x00000000 05 00
Sun Apr 16 22:08:12 2023 [INFO] Size: 0x004c (76)
Sun Apr 16 22:08:12 2023 [INFO] Unknown:
Sun Apr 16 22:08:12 2023 [INFO] 0x00000000 00 00 00 00
Sun Apr 16 22:08:12 2023 [INFO] Flags: 0x7 (7)
Sun Apr 16 22:08:12 2023 [INFO] Convert Log offset: 0x0000000000000
Sun Apr 16 22:08:12 2023 [INFO] Convert Log size:   0x00000000 (0)
Sun Apr 16 22:08:12 2023 [INFO] Sector size (1): 0x200 (512)
Sun Apr 16 22:08:12 2023 [INFO] Sector size (2): 0x200 (51
Sun Apr 16 22:08:12 2023 [INFO] ==========  ========  ====
Sun Apr 16 22:08:12 2023 [INFO] No clear key found.
```

```
X:\Windows\System32>manage-bde.exe -status d:
BitLocker Drive Encryption: Configuration Tool version 10.0.17134
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume D: [Label Unknown]
[Data Volume]

    Size:                 Unknown GB
    BitLocker Version:    2.0
    Conversion Status:    Unknown
    Percentage Encrypted: Unknown%
    Encryption Method:    XTS-AES 128
    Protection Status:    Unknown
    Lock Status:          Locked
    Identification Field: Unknown
    Automatic Unlock:     Disabled
    Key Protectors:
        TPM
        Numerical Password
```

Agenda Day 1

- ✓ Equipment Inspection
- ✓ Soldering Theory & Lab
- ✓ Tamper Protection Switches
- ✓ Forensic Data Acquisition
  - Notebook Internals
  - Notebook Disassembly

Key Takeaways

- ✓ Ability to Solder
- ✓ Tamper Protection Switches
- ✓ Basic Forensic Data Acquisition

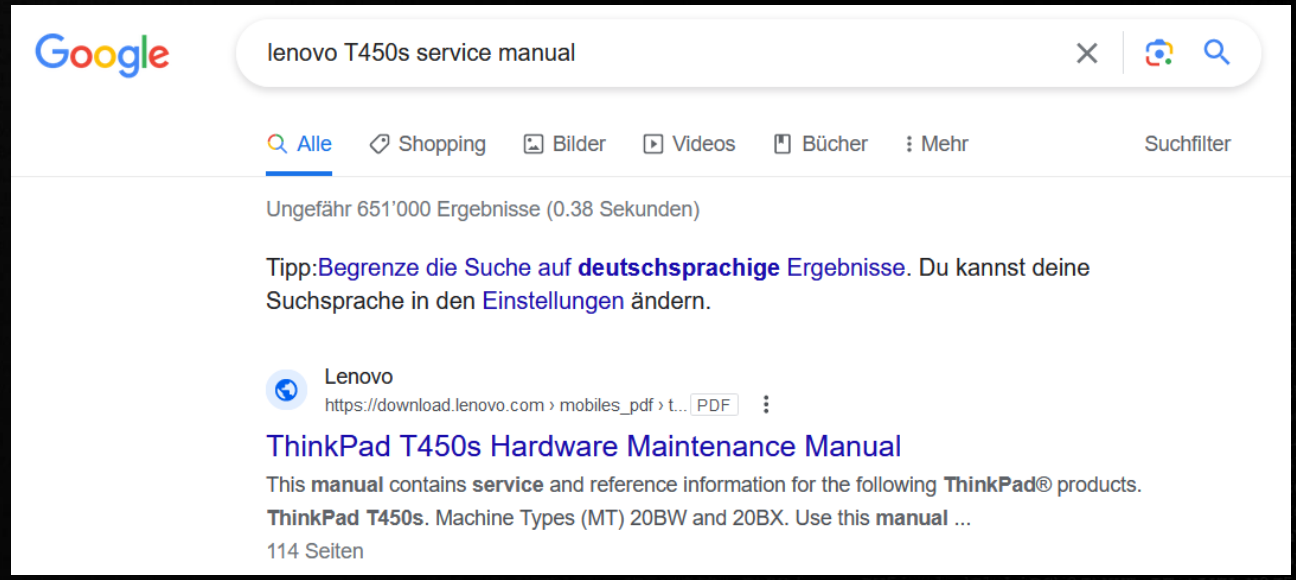
Mainboard Extraction Theory

- Search as much information about the target device as you can
- Vendor Service manuals
  - https://download.lenovo.com/pccbbs/mobiles_pdf/x260_hmm_en_sp40j47622_02.pdf
- Ifixit.com
- Test devices (ebay, resellers…)
- Google
- X-ray

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Mainboard Extraction Theory

- Service manuals
  - Searching with Google: “lenovo x260 service manual”



Mainboard Extraction Theory

Major FRUs

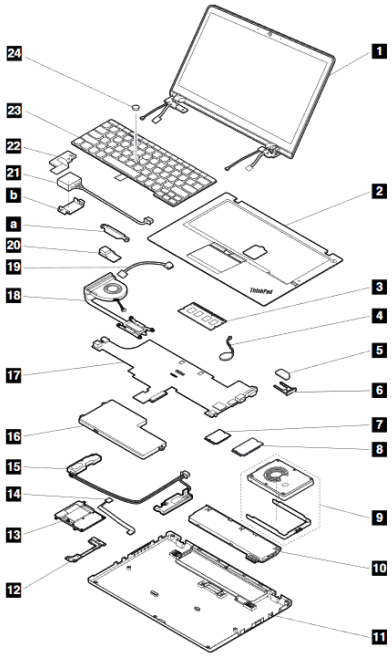


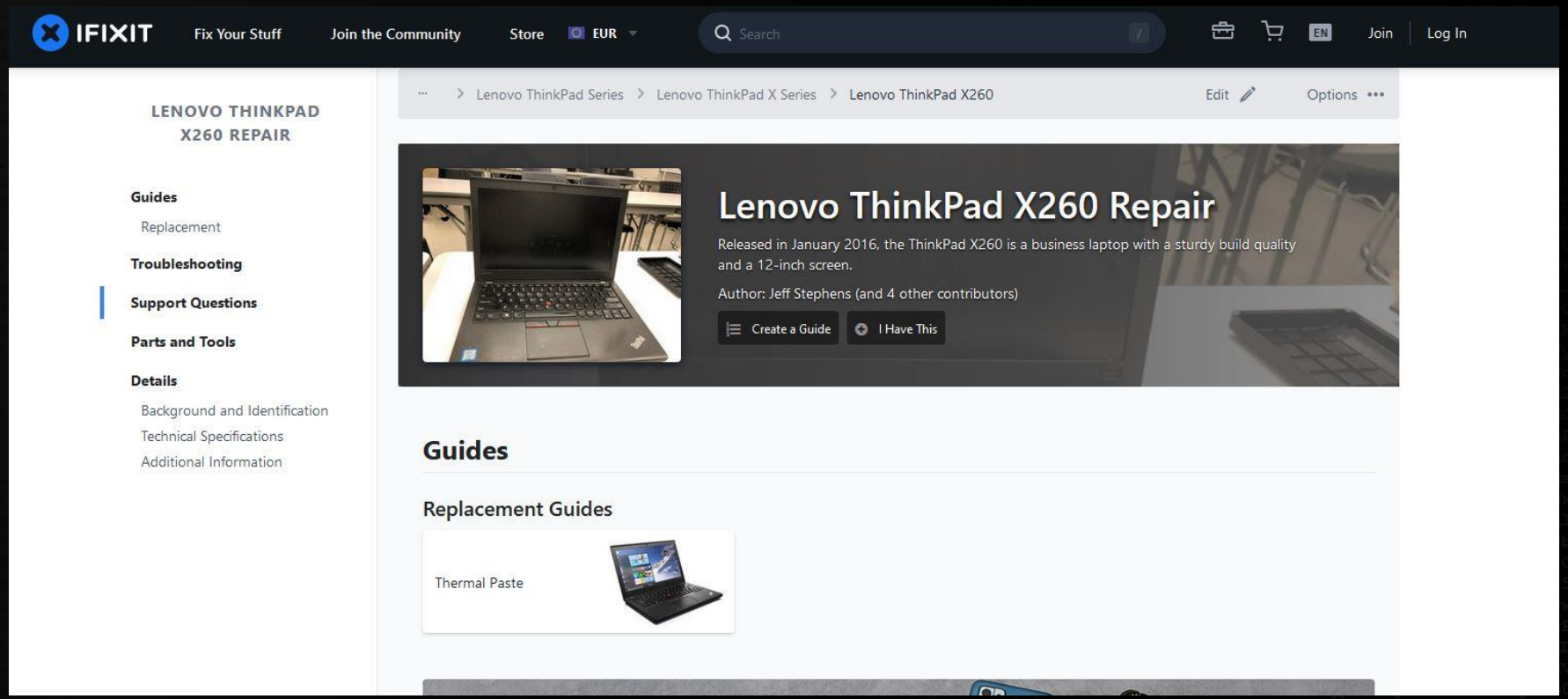
Table 9. Major FRUs

No.	FRU descriptions	Self-service CRU	Optional-service CRU
1	LCD unit	No	No
2	Keyboard bezel assembly	No	No
3	Memory module	No	Yes
4	Coin-cell battery	No	Yes
5	SIM card (available on some models)	Yes	No
6	SIM card tray	Yes	No
7	Wireless LAN card	No	Yes
8	Wireless WAN card or M.2 solid-state drive	No	Yes
9	Hard disk drive or solid-state drive (depending on the model)	No	Yes

https://download.lenovo.com/pccbbs/mobiles_pdf/x260_hmm_en_sp40j47622_02.pdf

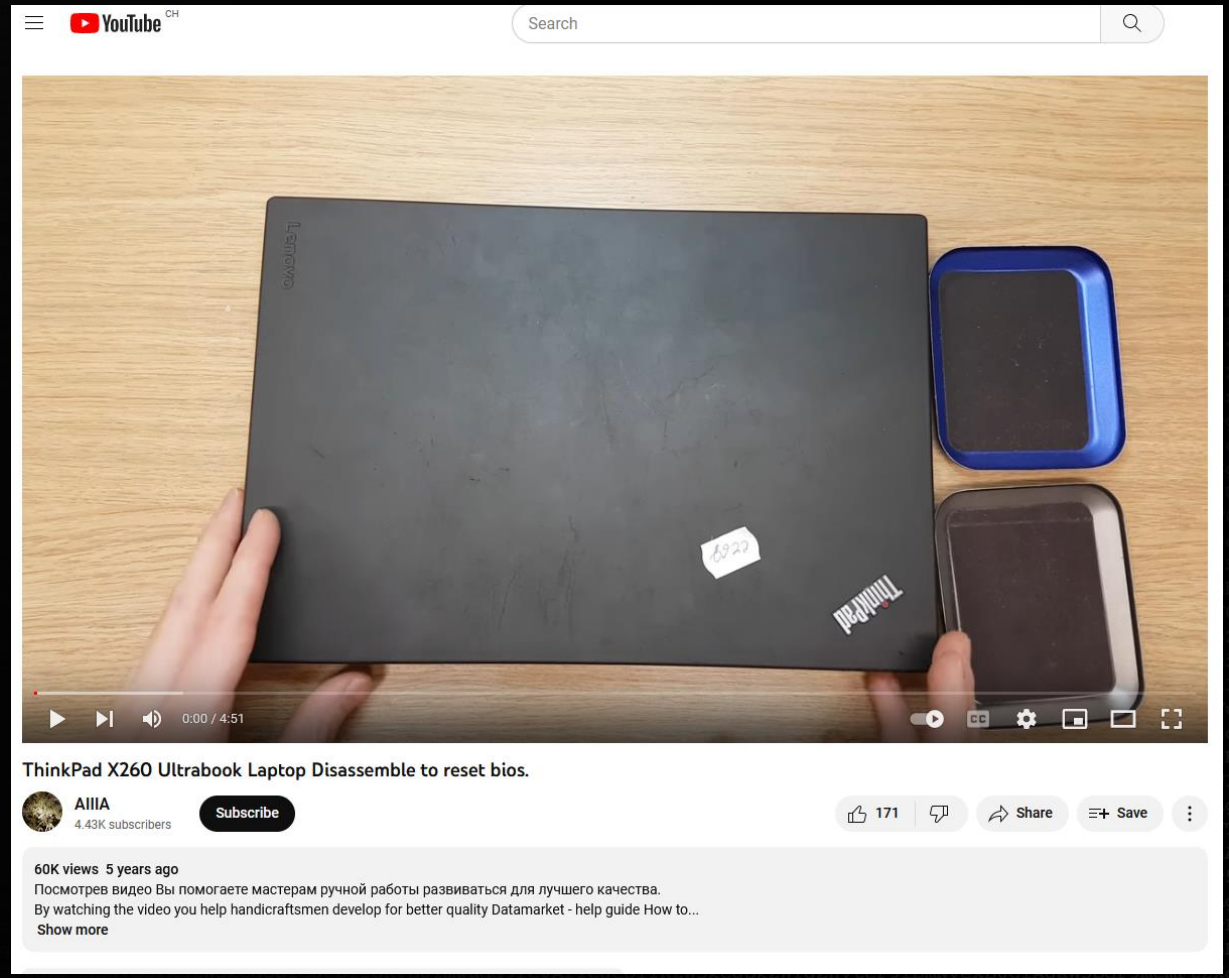
Mainboard Extraction Theory

- iFixit



Mainboard Extraction Theory

- YouTube
  - Search for:
    - “Lenovo x260 tear down”
    - “Lenovo x260 repair”
    - “Lenovo x260 disassemble”



Mainboard Extraction Theory

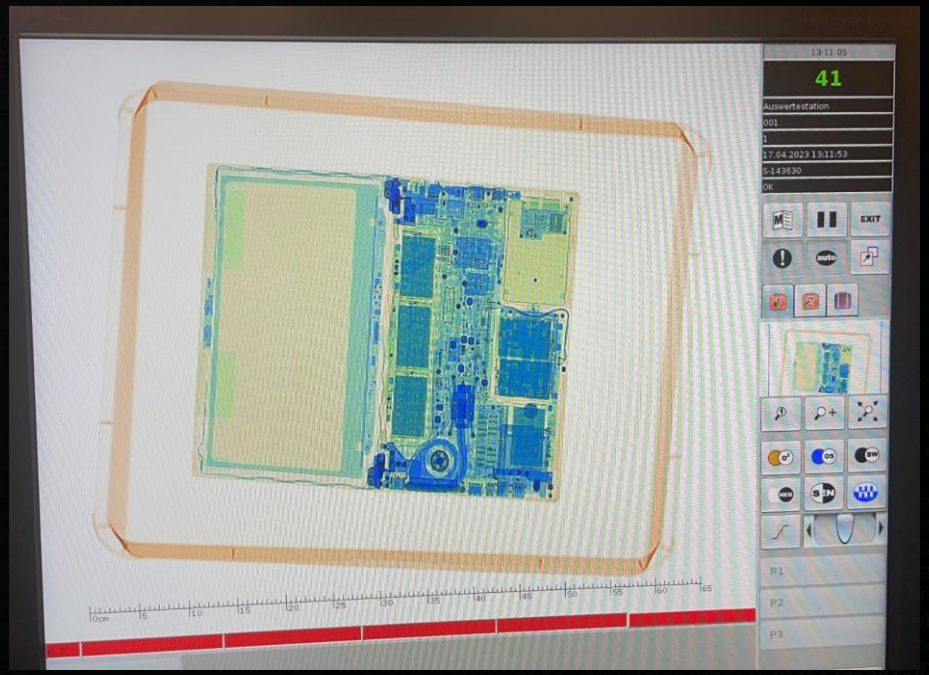
lumafield

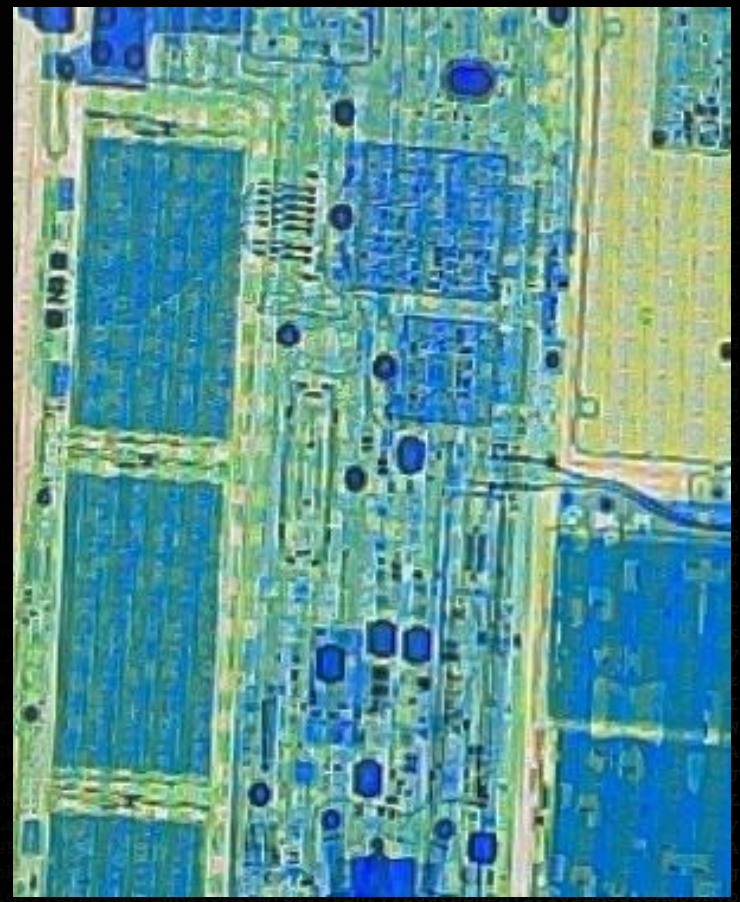
- X-Ray
  - stationary X-ray
  - mobile X-ray
- Lumafield etc.

https://www.lumafield.com/

Mainboard Extraction Theory

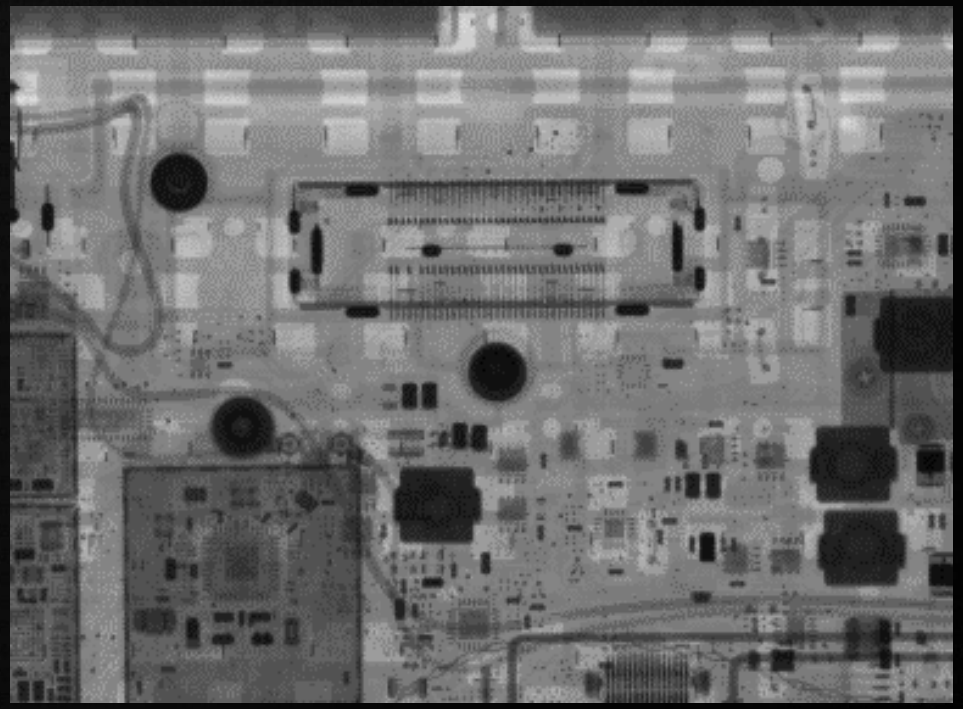
- Security control
  - Mostly a bad resolution

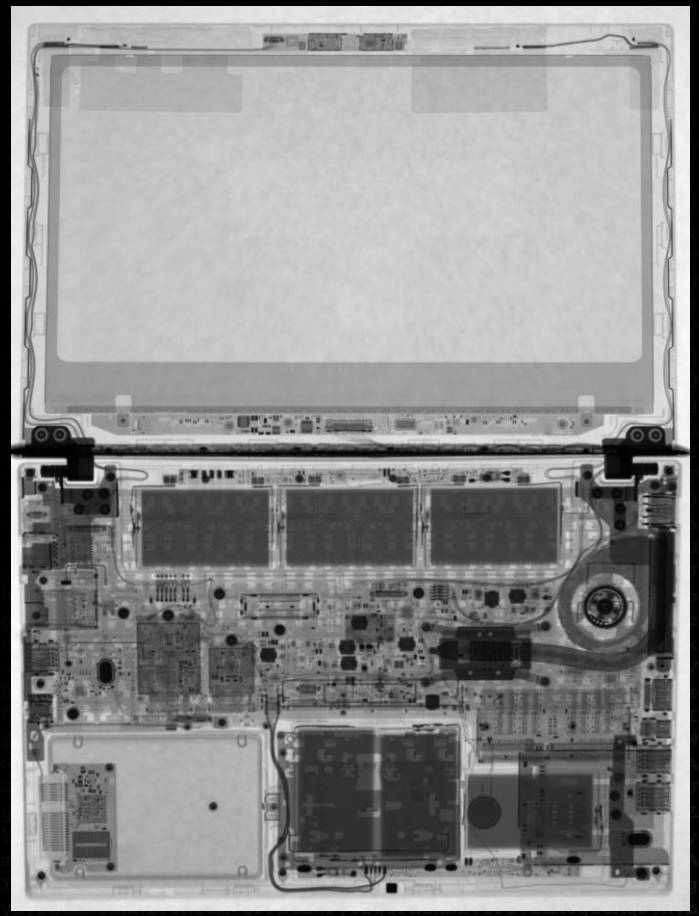




Mainboard Extraction Theory

- High Resolution X-Ray Machines preferred





black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

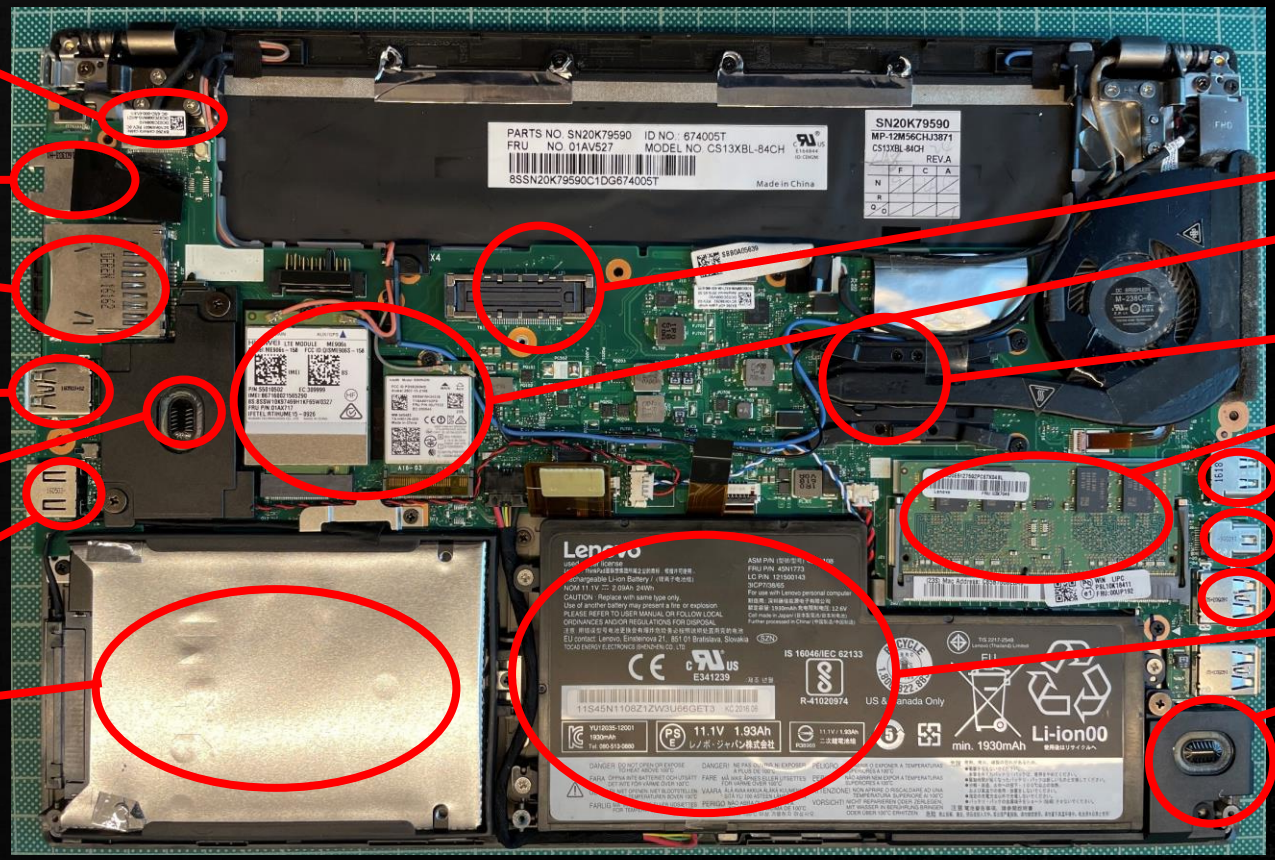
Coffee Break

Mainboard Extraction

- Carefully remove the black plastic cover

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Notebook Internals



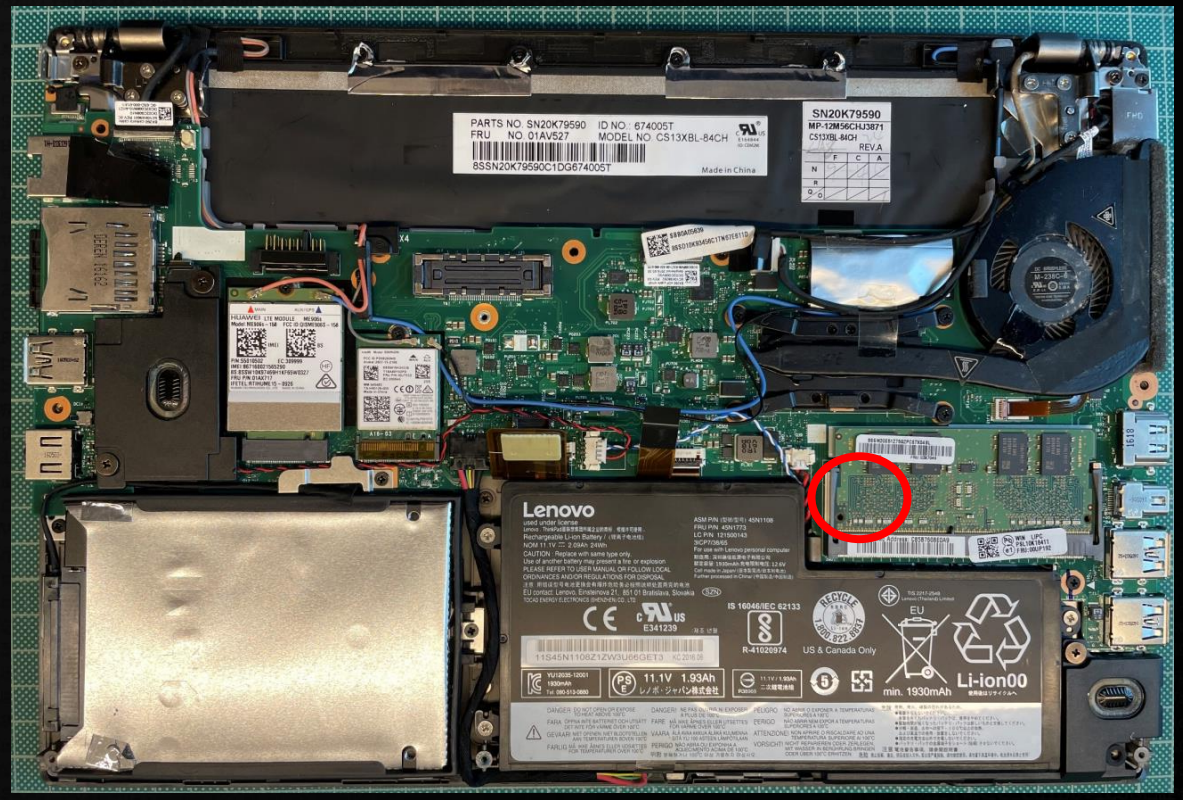
- Internal Display
- Network connection
- SD-Card & SIM-Card
- USB connector
- Speaker
- Audio
- HDD / SSD

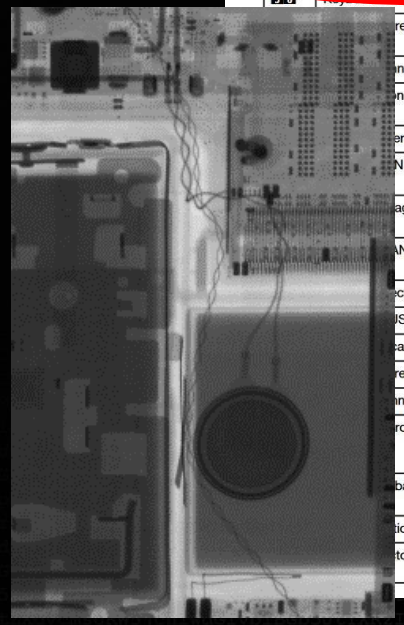
- Dockingstation
- Additional PCI Wi-Fi and GSM Cards
- CPU with Heatpipe / Fan
- RAM
- HDMI
- Displayport
- USB connector
- Internal Battery
- Speaker

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

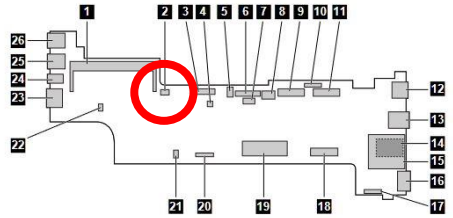
Bios Buffer Battery

- Coin-cell battery connector **(do not disconnect!)**





System board connectors and cables



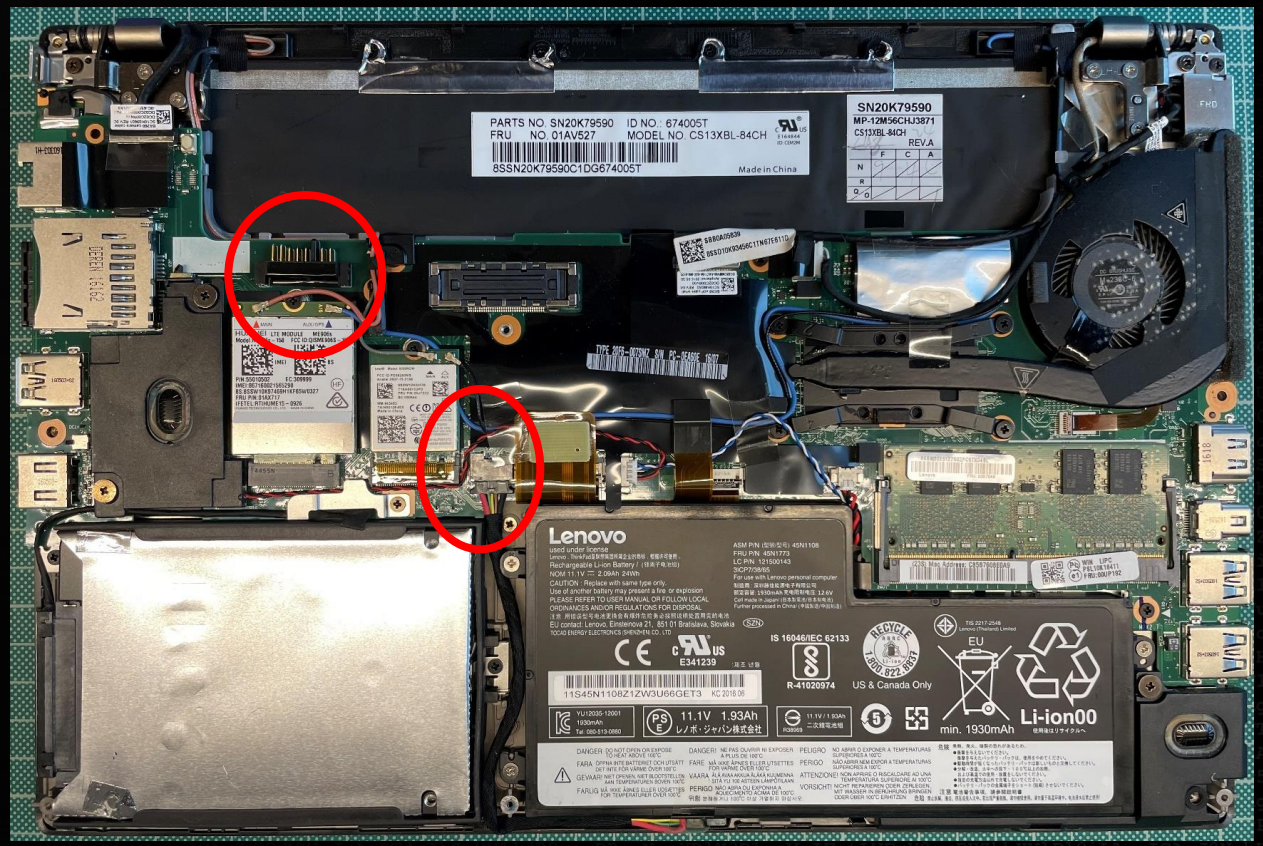
No.	Connector/location	Internal cable
1	Memory module slot (internal)	None, with the memory module directly connecting to the system board
2	Coin-cell battery connector (internal)	Coin-cell battery with cable
3, 6	[illegible]	Keyboard assembly with cables
	reader connector (internal)	FPC for smart-card reader, connecting the smart-card reader to the system board
	nector (internal)	Speaker assembly with cable
	nnector (internal)	FPC for trackpad, connecting the trackpad to the system board
	ery connector (internal)	Built-in battery assembly with cable
	N card or WiGig module slot (internal)	None, with the wireless-LAN card or WiGig module directly connecting to the system board
	age-drive connector (internal)	Internal-storage-drive cable, connecting the internal storage drive to the system board
	AN card slot (internal)	None, with the wireless-WAN card directly connecting to the system board
	ctor (right side)	None. Integrated.
	SB 3.0 connector (right side)	None. Integrated.
	ard reader (right side)	None. Integrated.
	reader (right side)	None. Integrated.
	nector (right side)	None. Integrated.
	rophone module connector (internal)	Camera cable, connecting the camera/microphone module, the power-button card, and the ThinkPad logo LED (on the A-cover) to the system board
	battery connector (internal)	None, with the removable battery directly connecting to the system board
	ion connector (bottom)	None. Integrated.
	tor (internal)	LCD cable, connecting the LCD unit to the system board

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Mainboard Extraction

Danger Zones!

- Only use plastic spatula when working on the mainboard



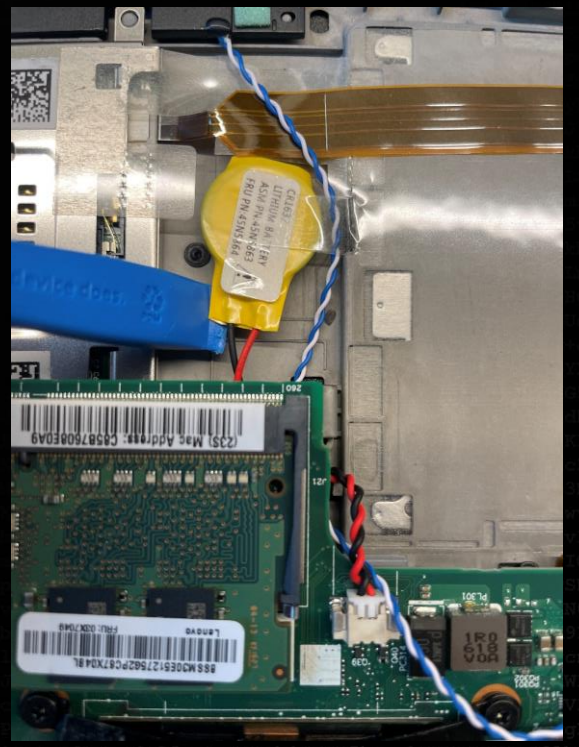
black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Mainboard Extraction

- Let‘s remove the internal battery

Mainboard Extraction

- Remove the coin-cell battery carefully from the housing
- Never disconnect the coin-cell battery!



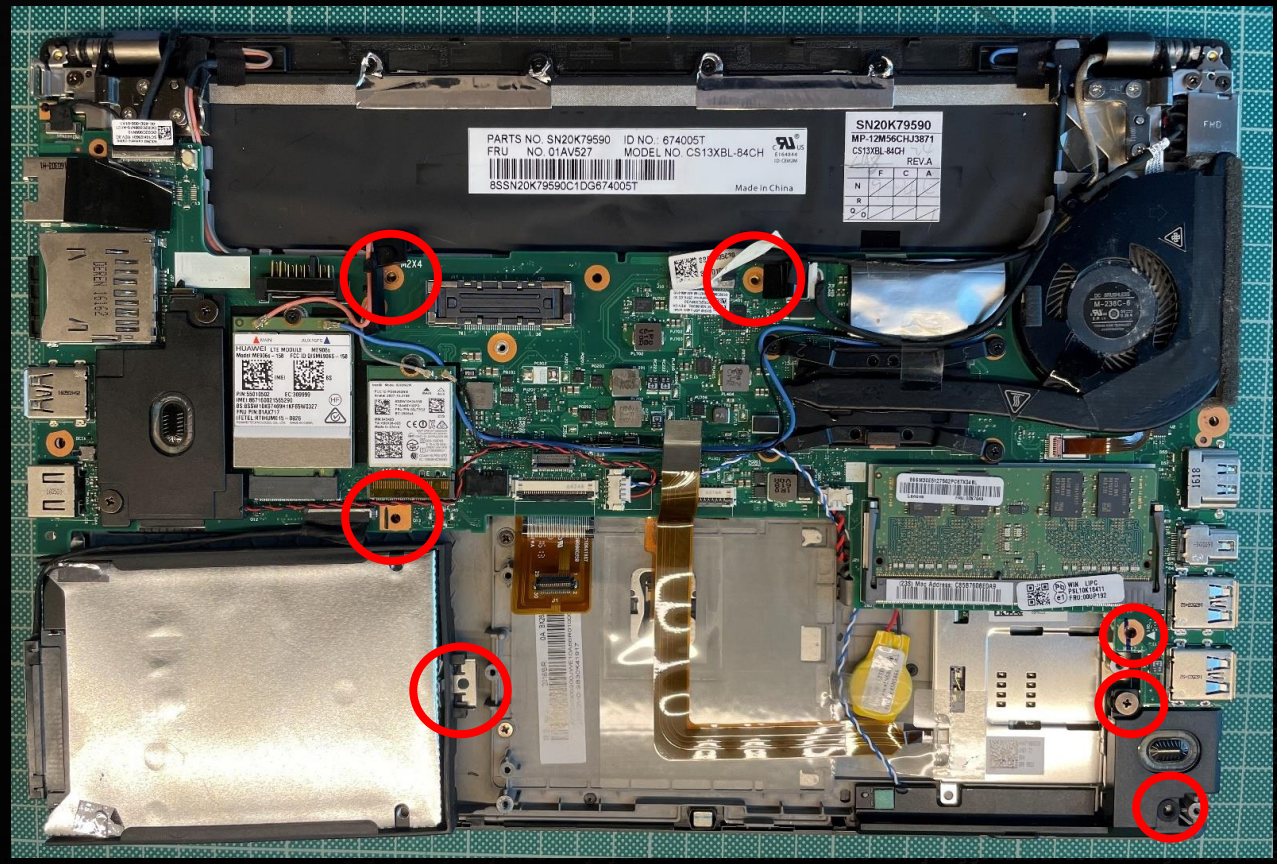
Mainboard Extraction

- Disconnect the necessary micro-plugs and flat ribbon cable from the board (not the one from the coin-cell battery ;-))

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Mainboard Extraction

- Remove all the marked screws



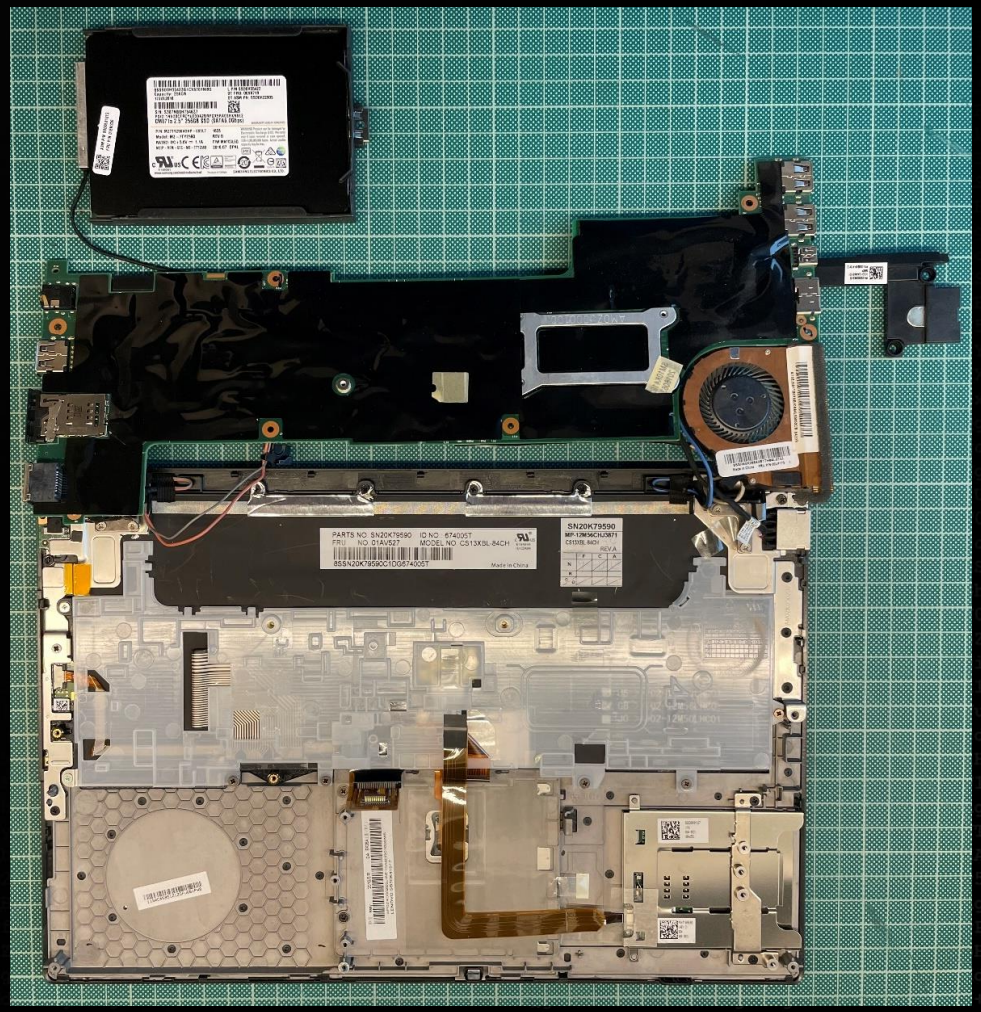
Mainboard Extraction

- Check that all the wires are disconnected and can freely move

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

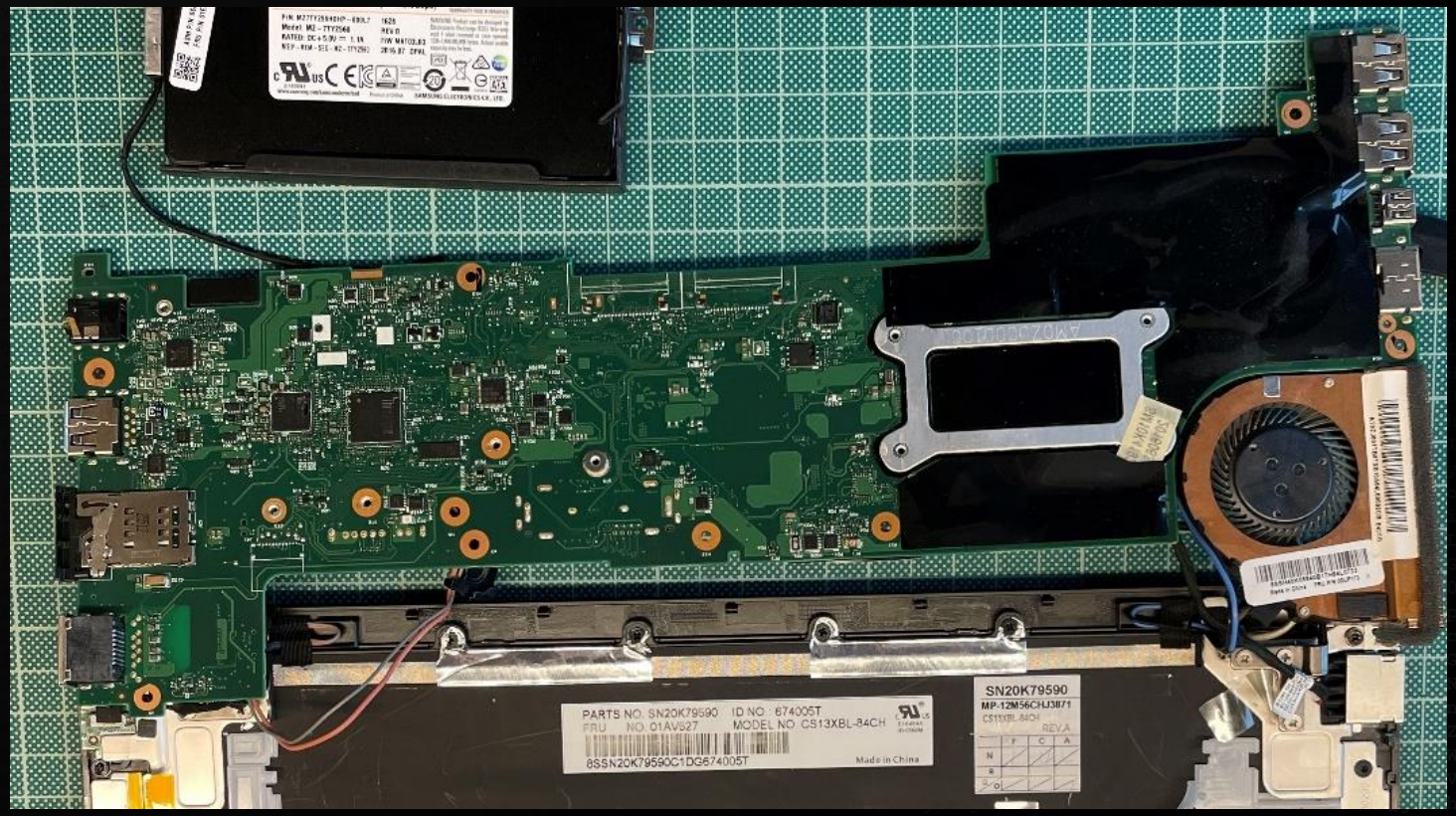
Mainboard Extraction

- Carefully remove the mainboard
- Take attention to the cable
- Do not disconnect the cell-coin battery



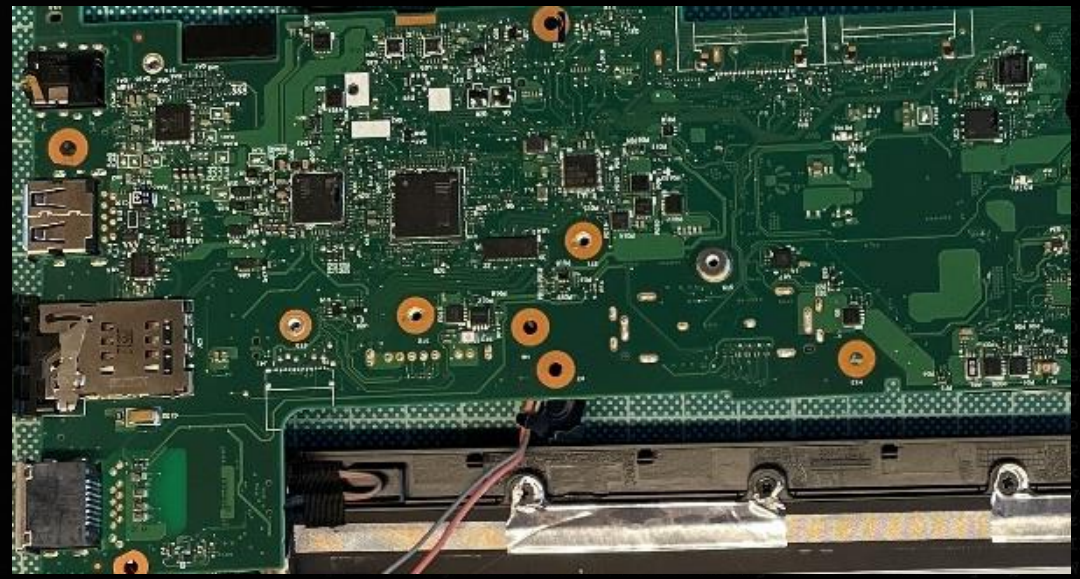
Mainboard Extraction

- Carefully remove the plastic cover



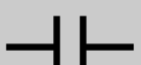
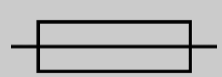
Mainboard Components

- Different Component Types
- Finding Repair Documentation
- Reading Schematics
- Working with Board View Data



black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Passive Components

Resistors	Capacitors	Inductors	Diodes	Crystals	Fuses
R1, R2, R3 …	C1, C2, C3 …	L1, L2, L3 …	D1, D2, D3 …	X1, X2, X3 …	F1, F2, F3 …
Ω	F	H	n/a	Hz	A
					
					

https://www.kicad.org/

Different SMD Chip Packages

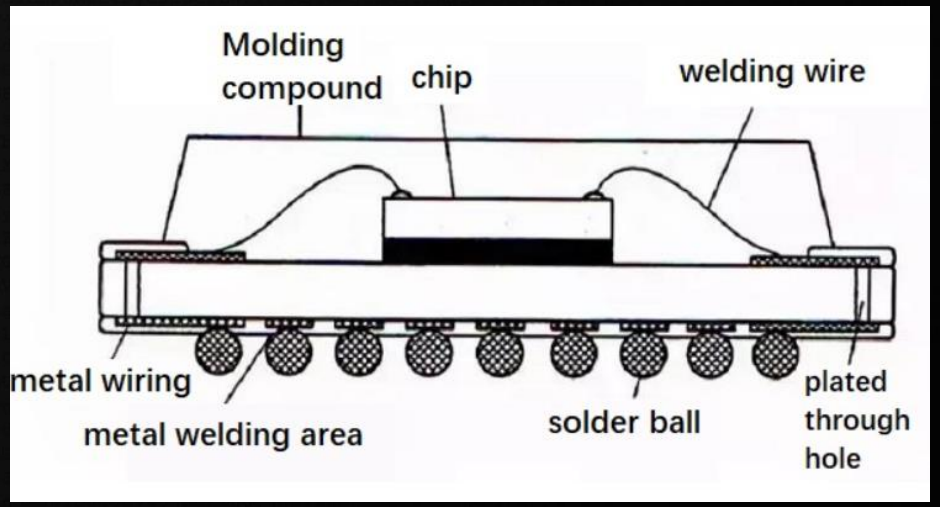
Attribute	SOIC-20 (DW)	SSOP-20 (DB)	TSSOP-20 (PW)	TVSOP-20 (DGV)	QFN-20 (RGY)
Length, mm	12.82 ±0.13	7.20 ±0.30	6.50 ±0.10	5.00 ±0.10	4.50 ±0.15
Width, mm	10.40 ±0.25	7.80 ±0.40	6.40 ±0.20	6.40 ±0.20	3.50 ±0.15
Height, Max. mm	2.65	2.00	1.20	1.20	1.00
Pitch, mm	1.27	0.65	0.65	0.40	0.50
Footprint, mm^2	133.33	56.16	41.60	32.00	15.75
Weight, g	0.495	0.151	0.075	0.055	0.043
Area savings, %	88.19	71.96	62.14	50.78	-

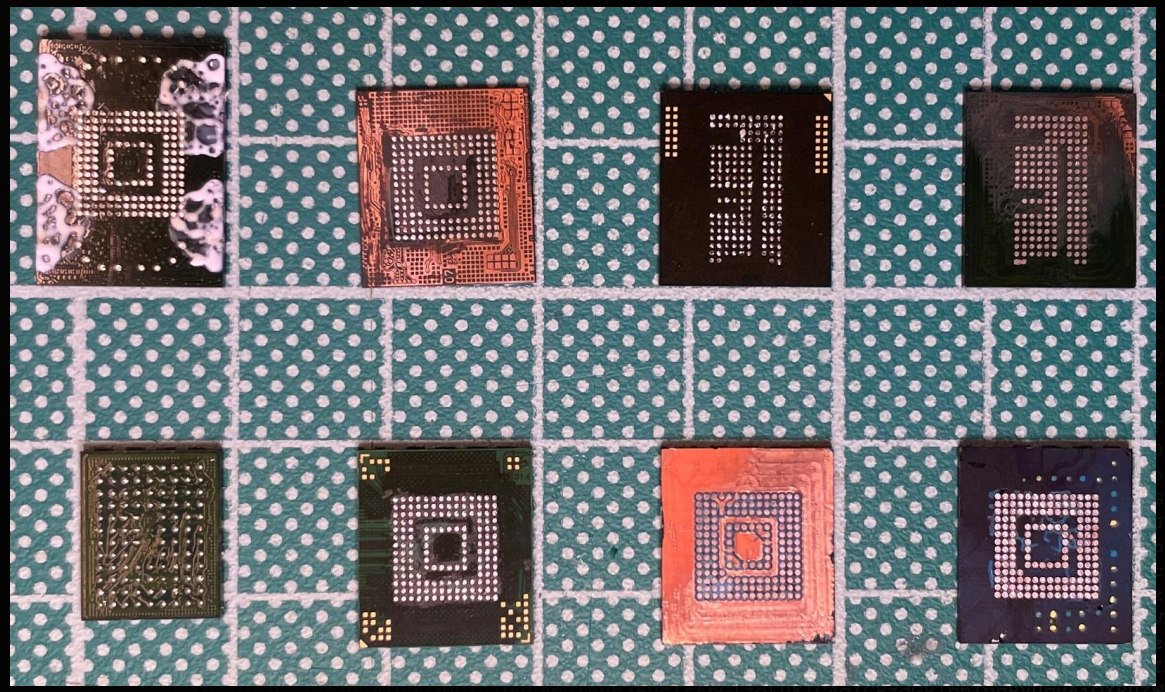
Figure 5. 20-Pin QFN Comparison to Alternative Package Solutions

https://www.ti.com/lit/an/scba017d/scba017d.pdf

Different SMD Chip Packages

- Typical BGA Chips

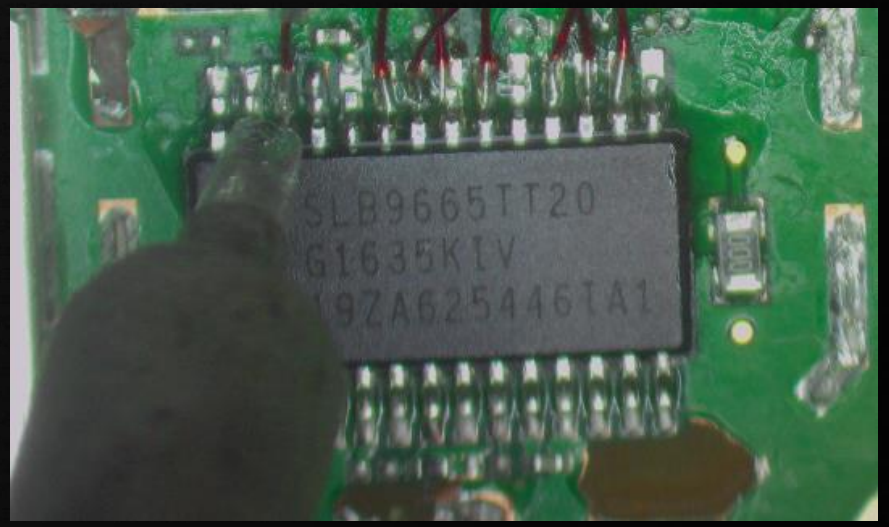


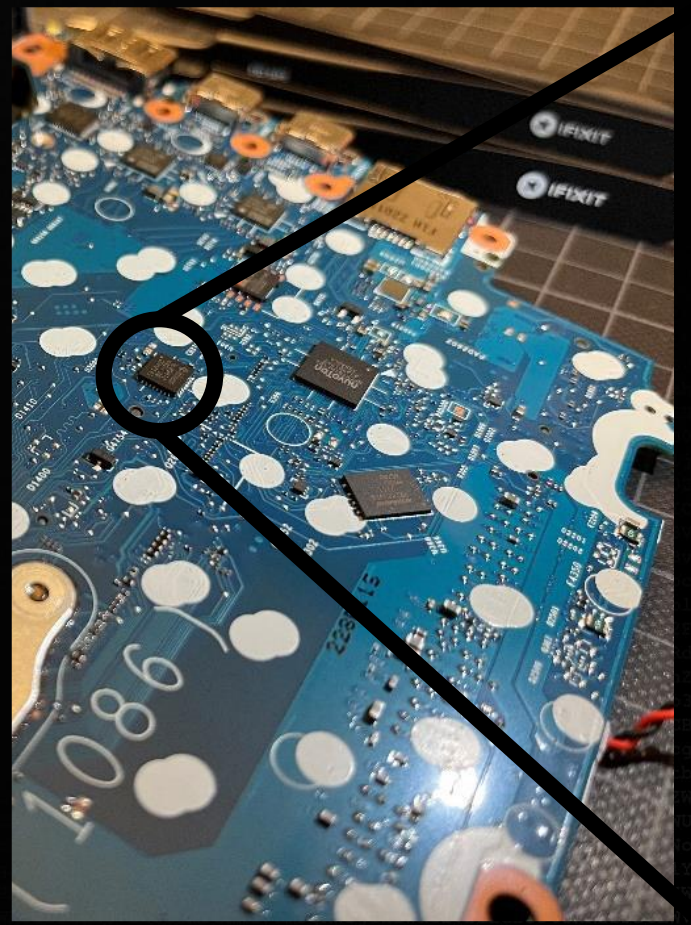


https://www.utmel.com/blog/categories/integrated%20circuit/introduction-to-bga-package

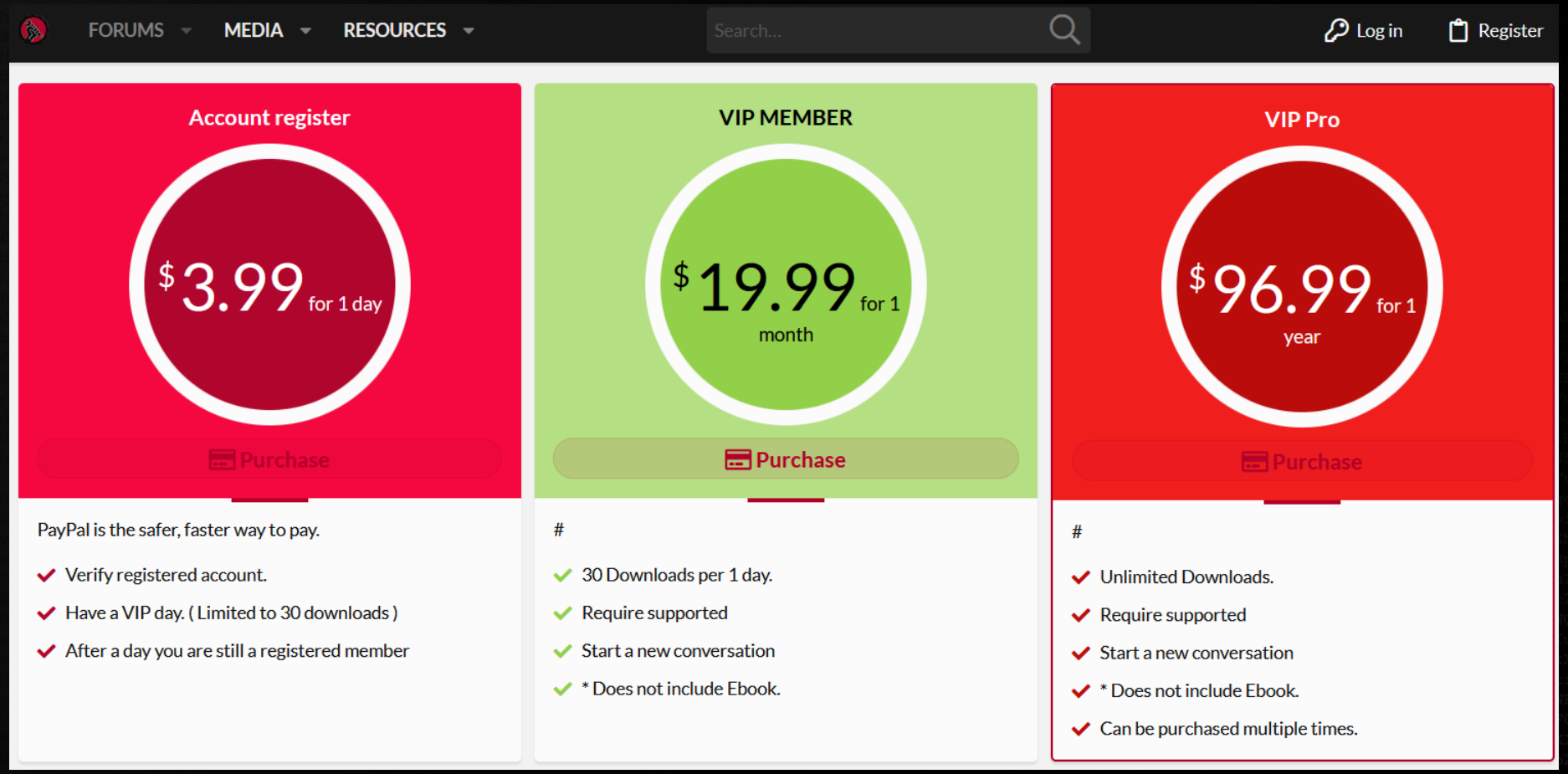
Identify Chips

- Google for name + datasheet
- Yandex might help



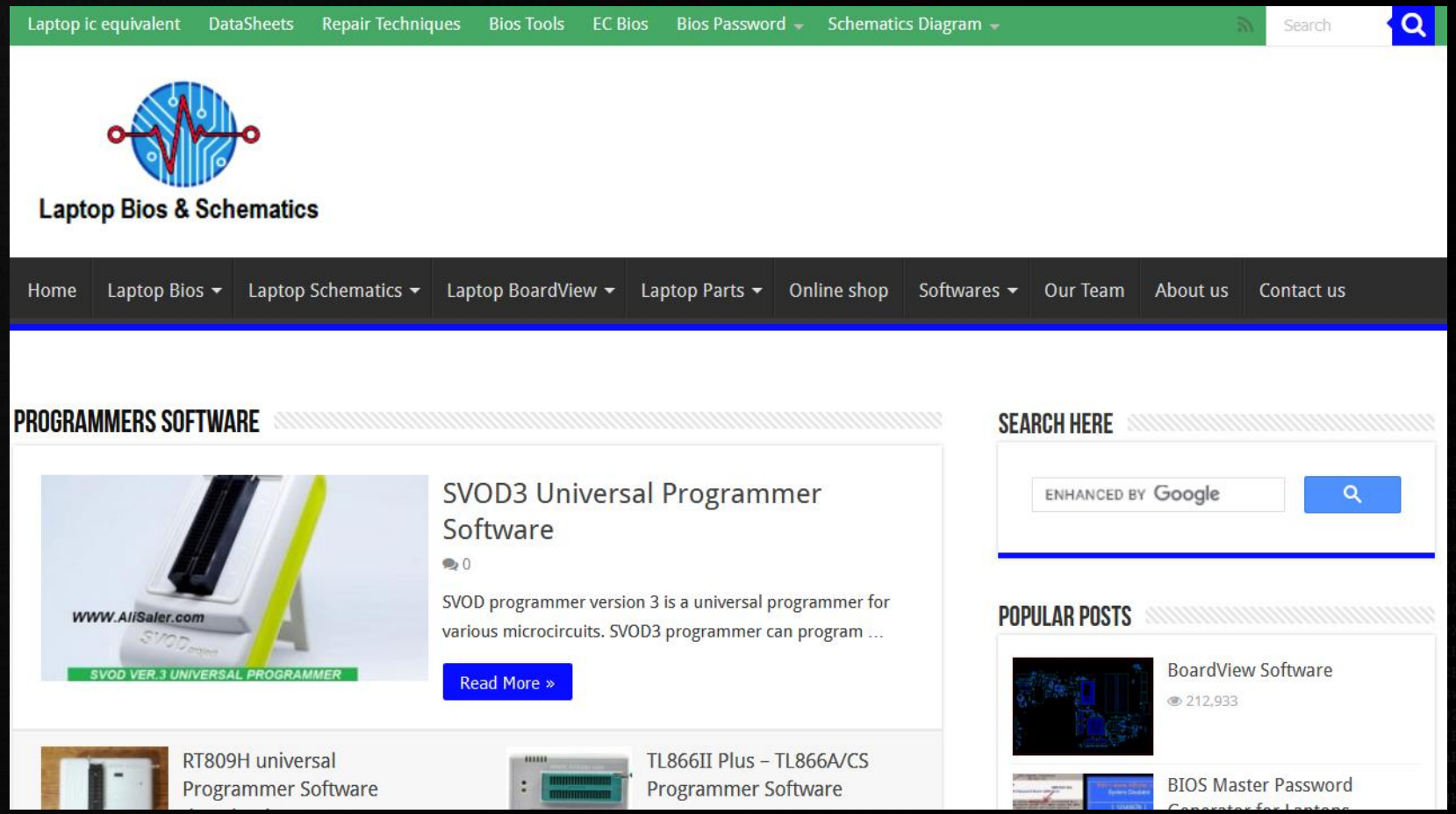


Finding Repair Documentation



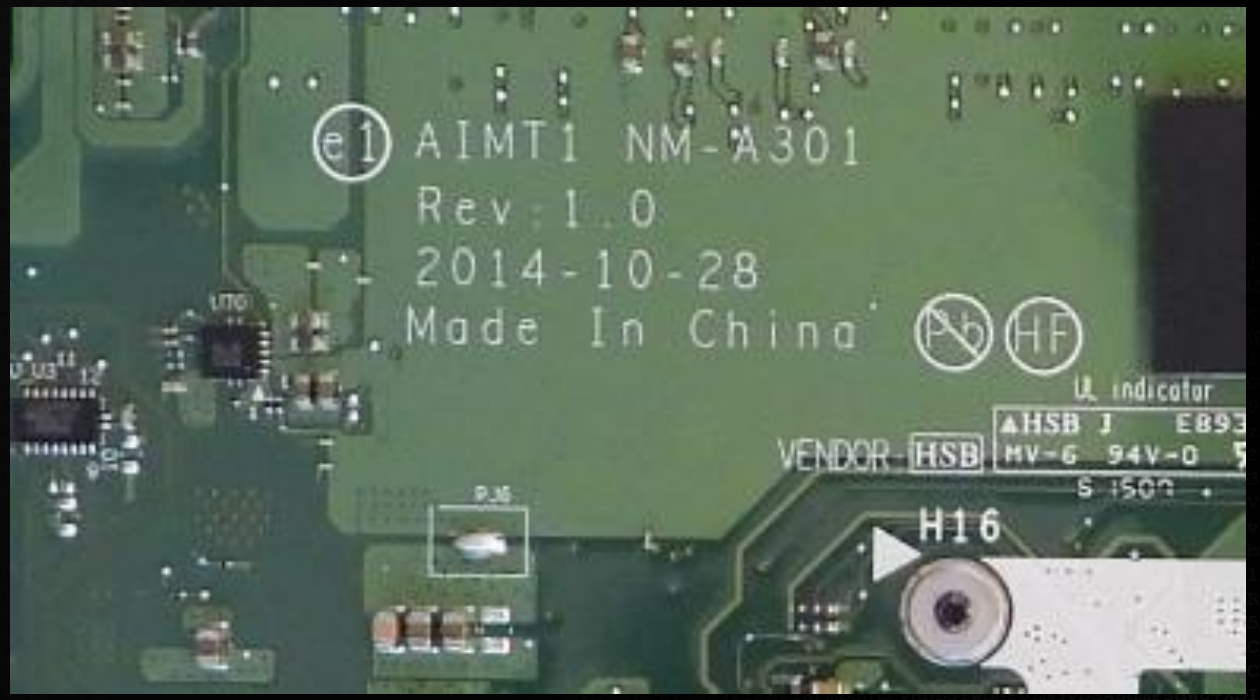
https://vinafix.com

Finding Repair Documentation



https://www.alisaler.com

Finding Repair Documentation

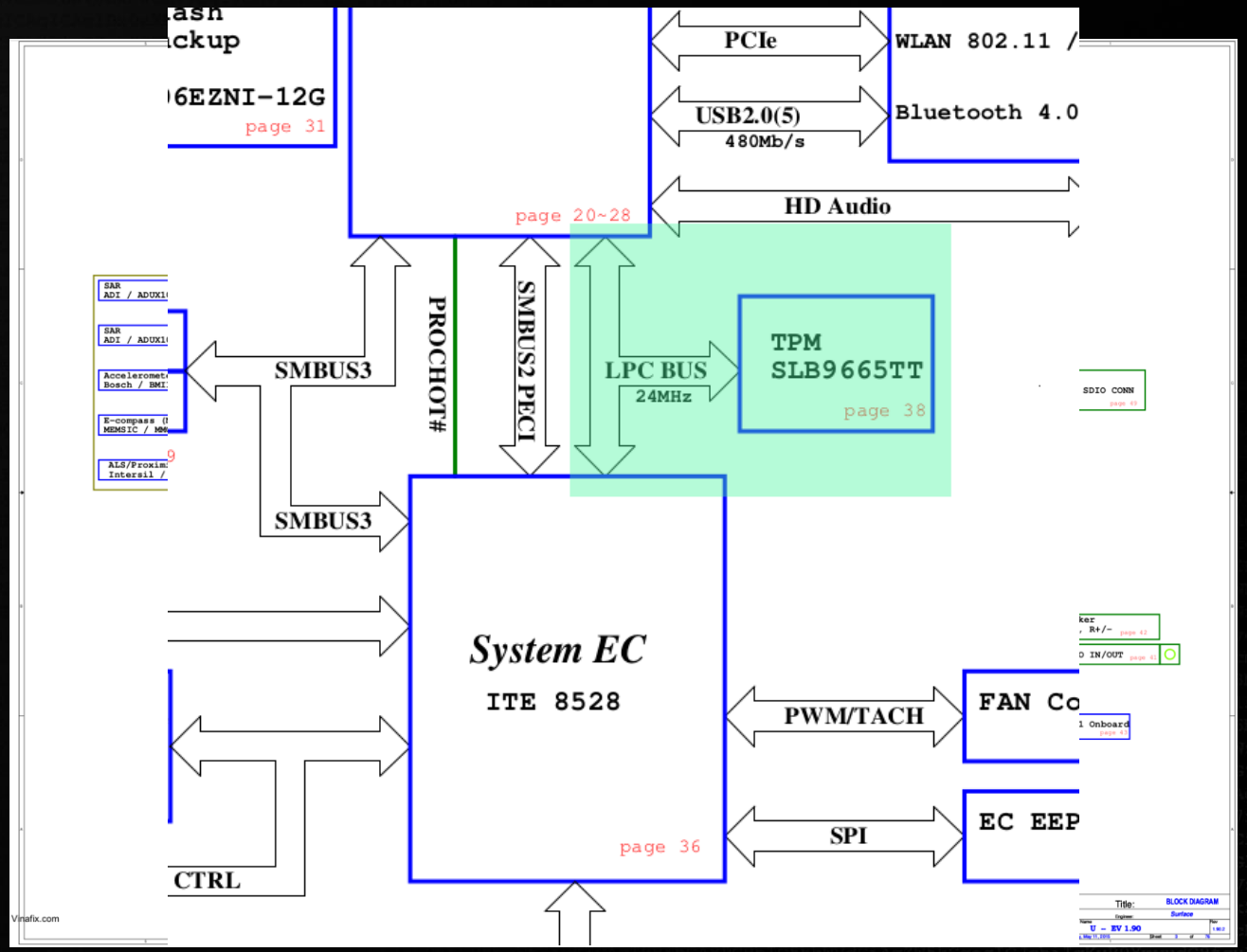


https://vinafix.com

Finding Repair Documentation

https://www.google.com

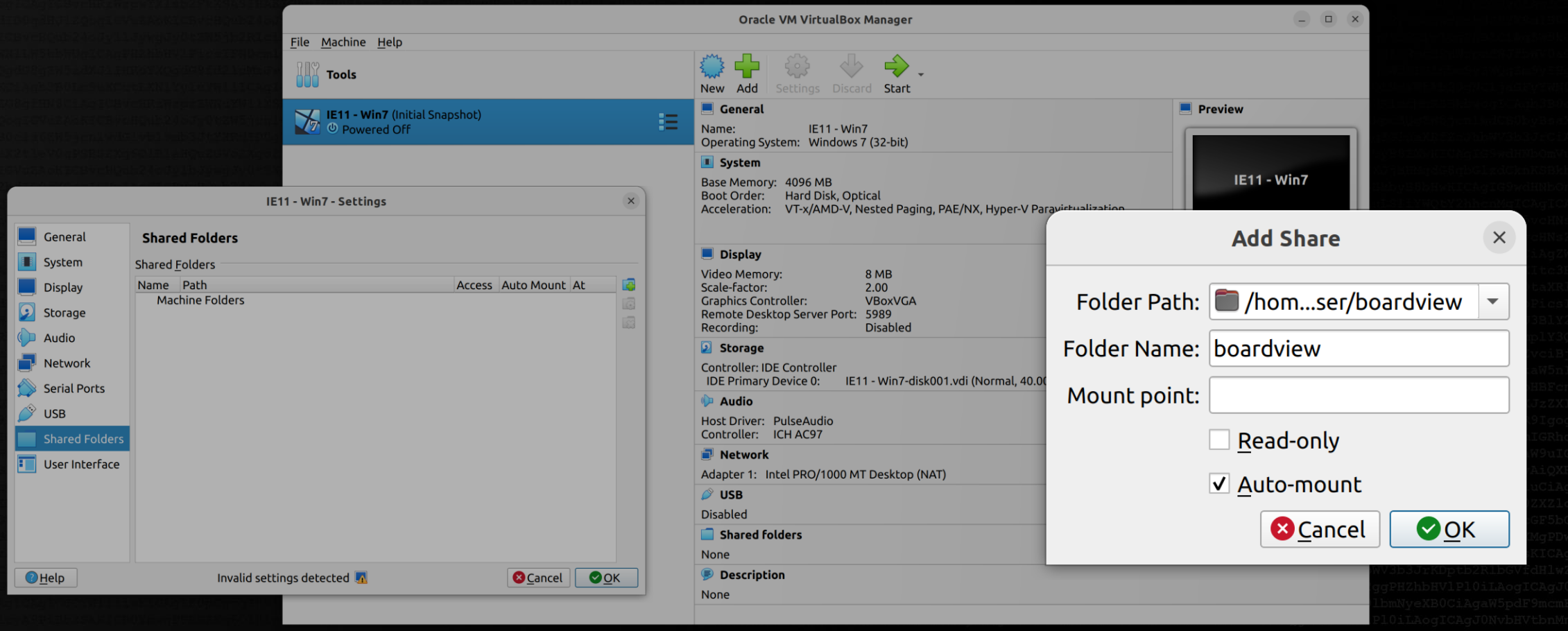
Identify Shared Bus Systems



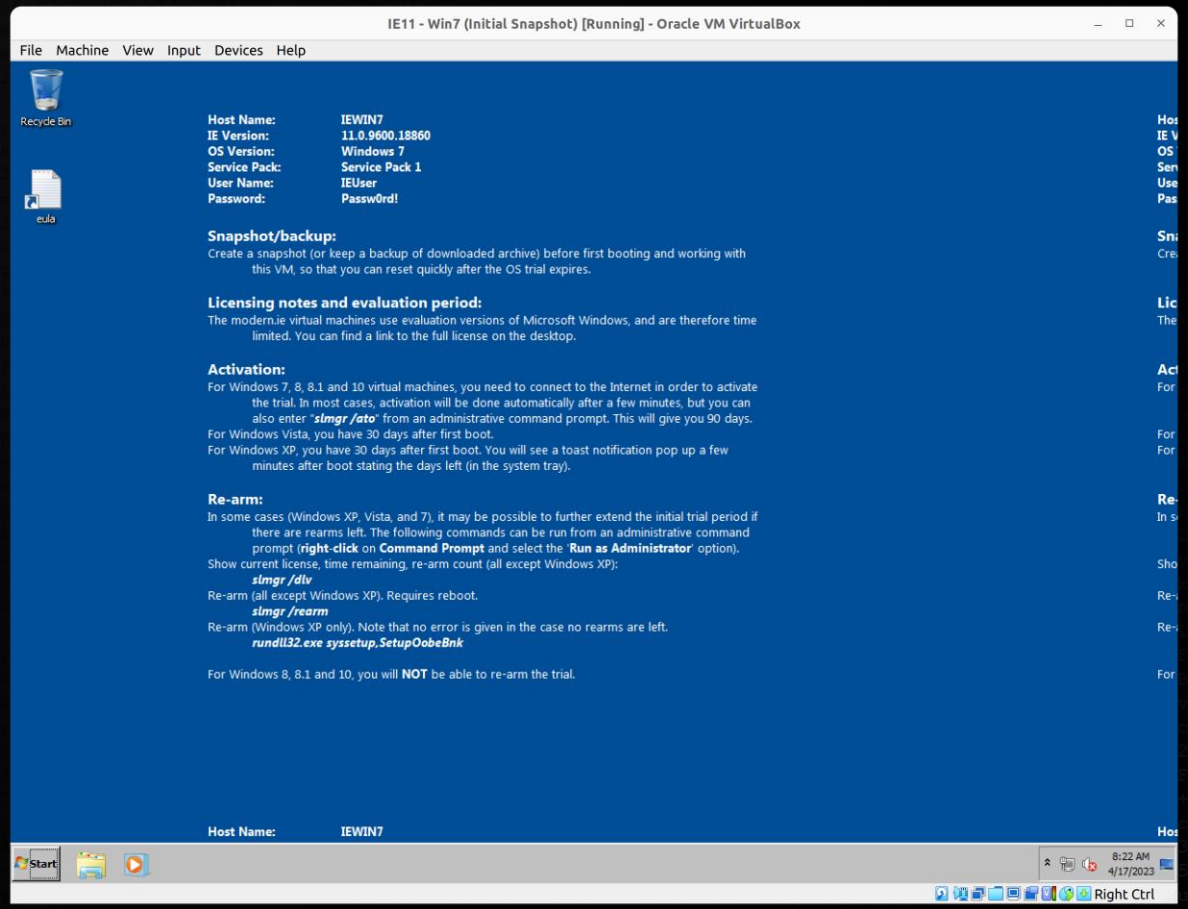
https://vinafix.com

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

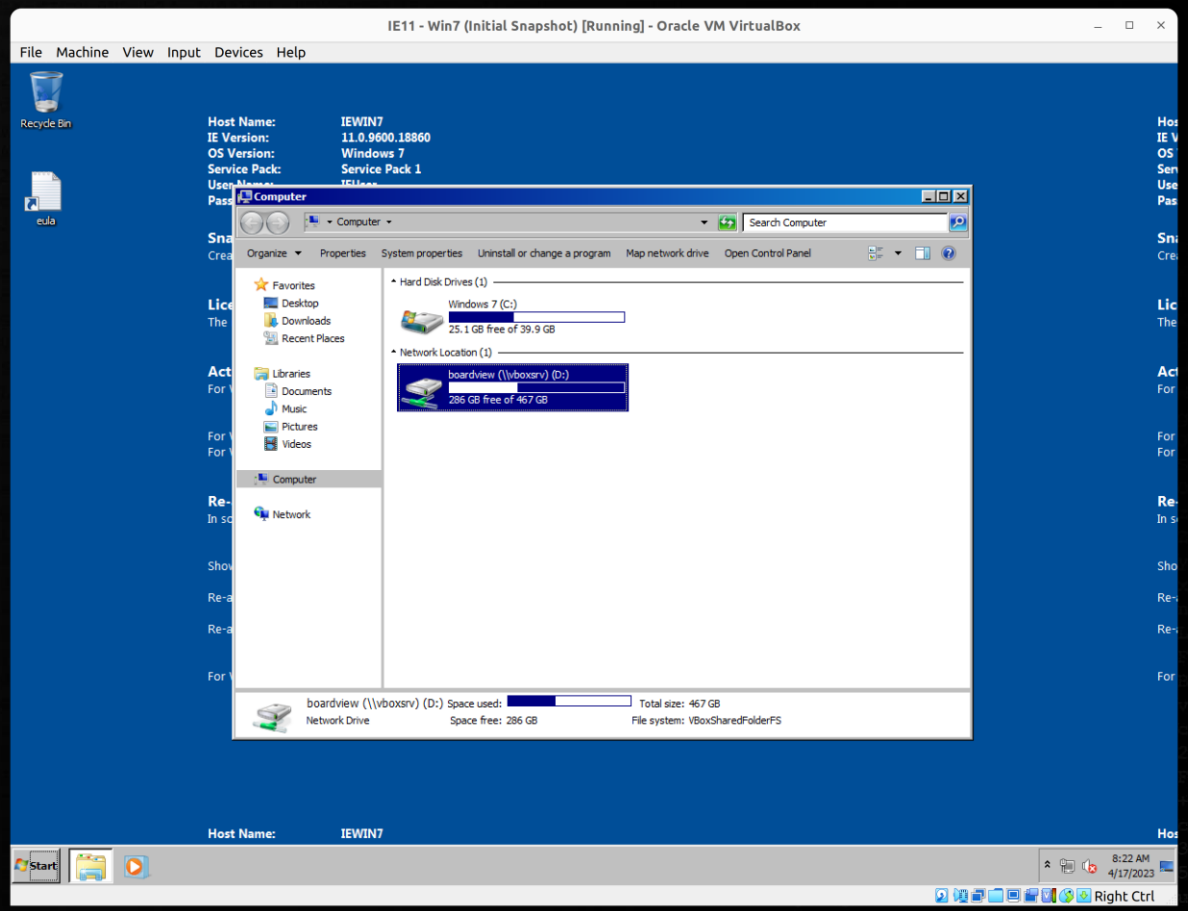
Board View Data



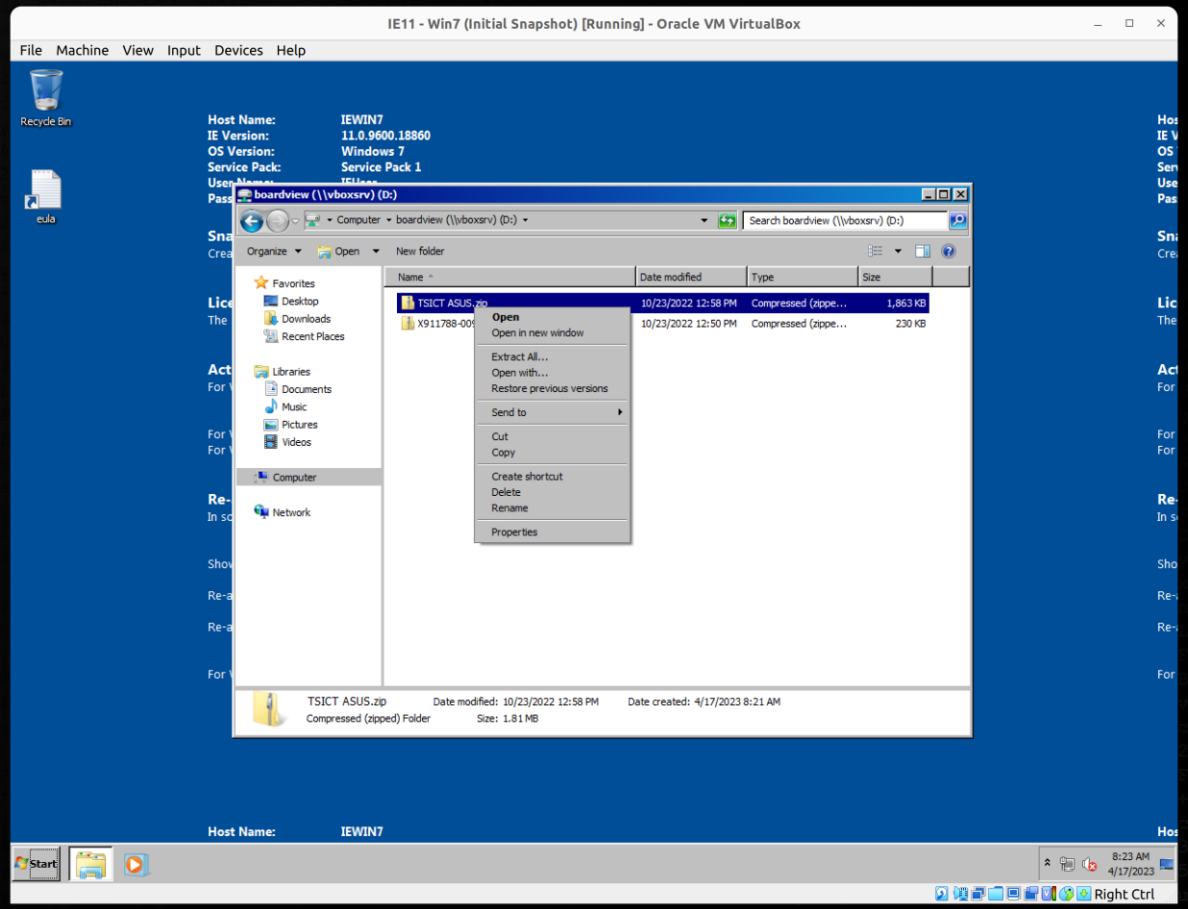
Board View Data



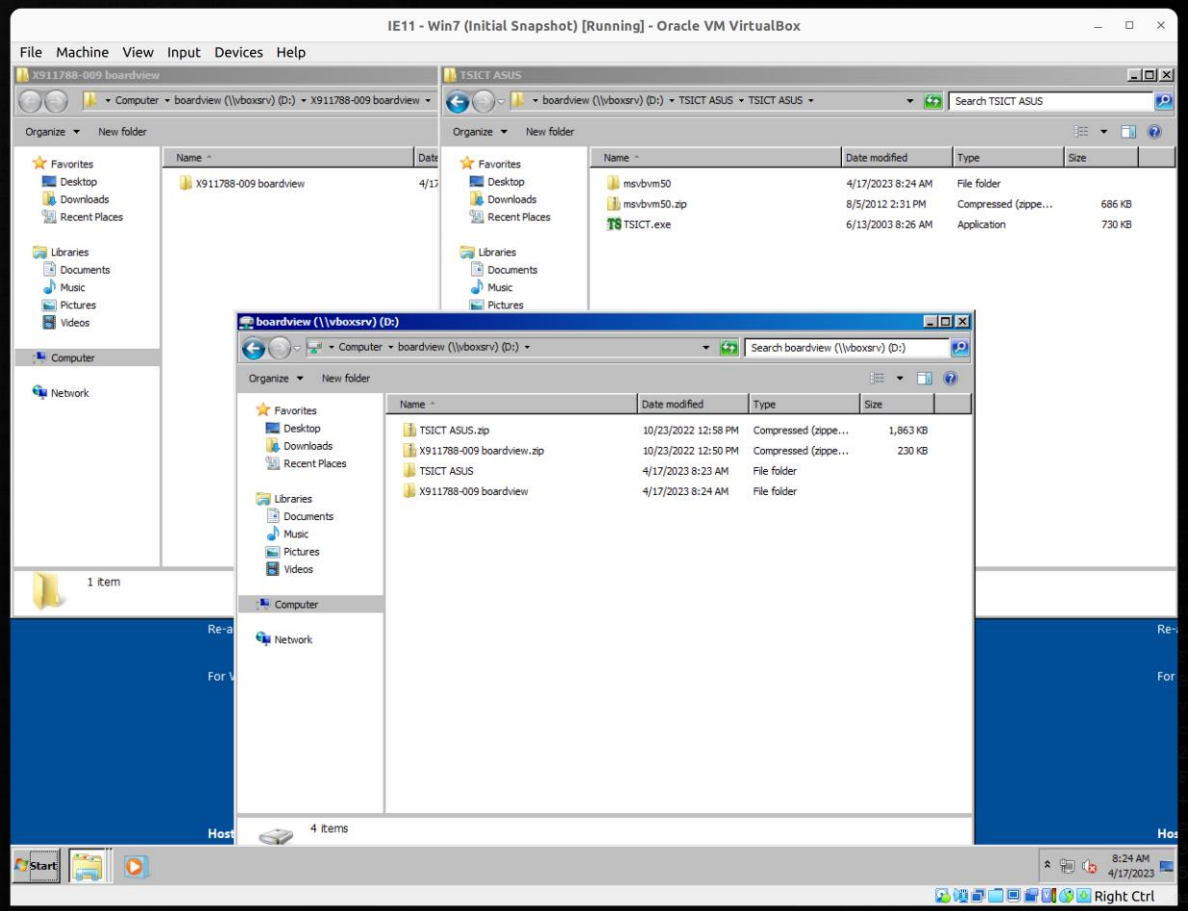
Board View Data



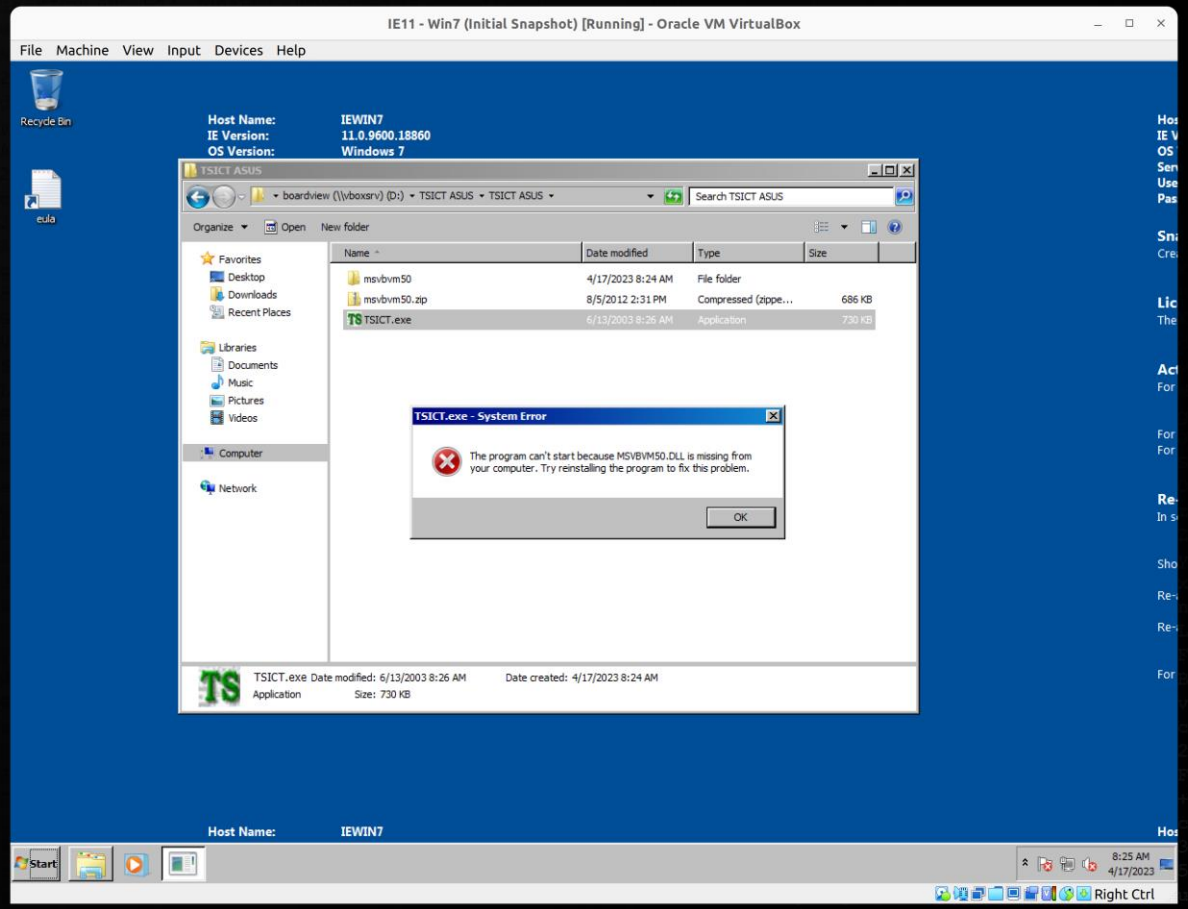
Board View Data



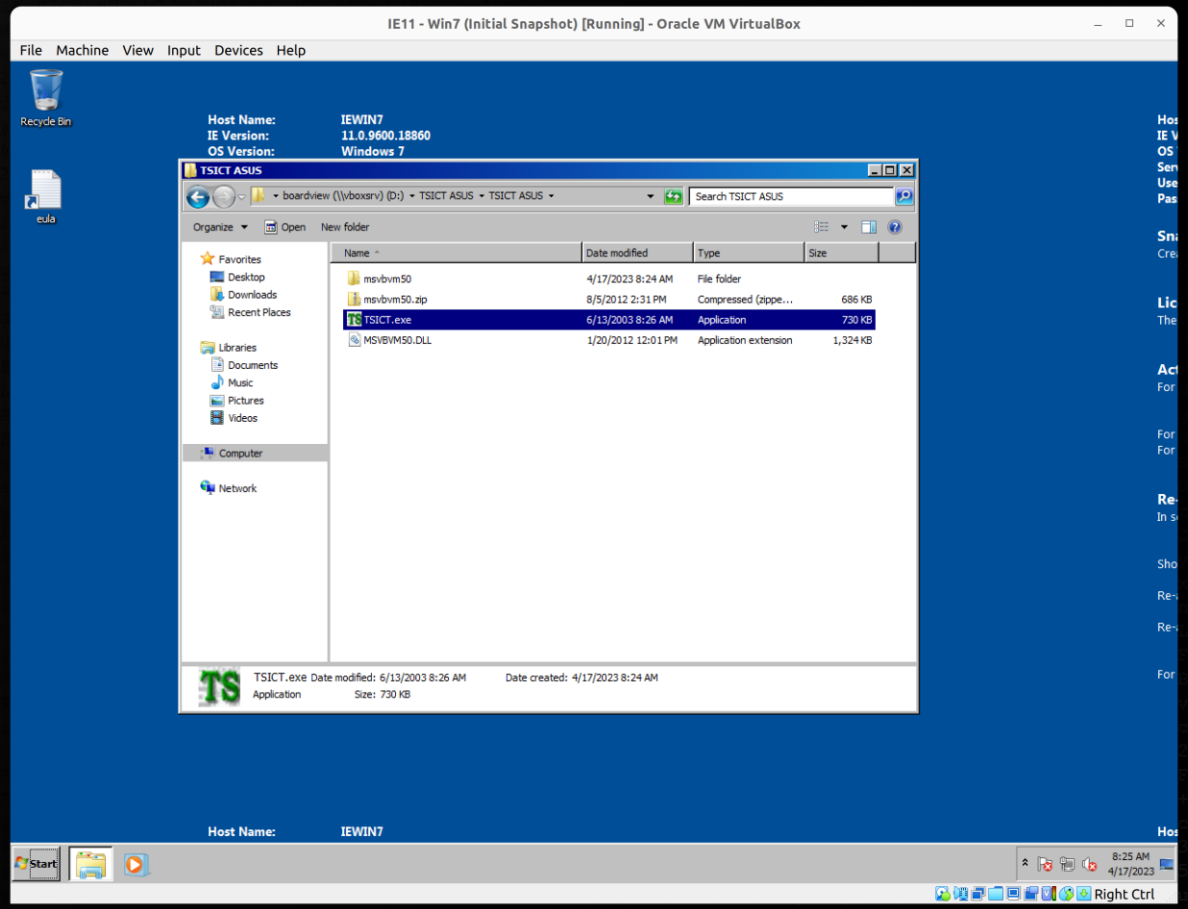
Board View Data



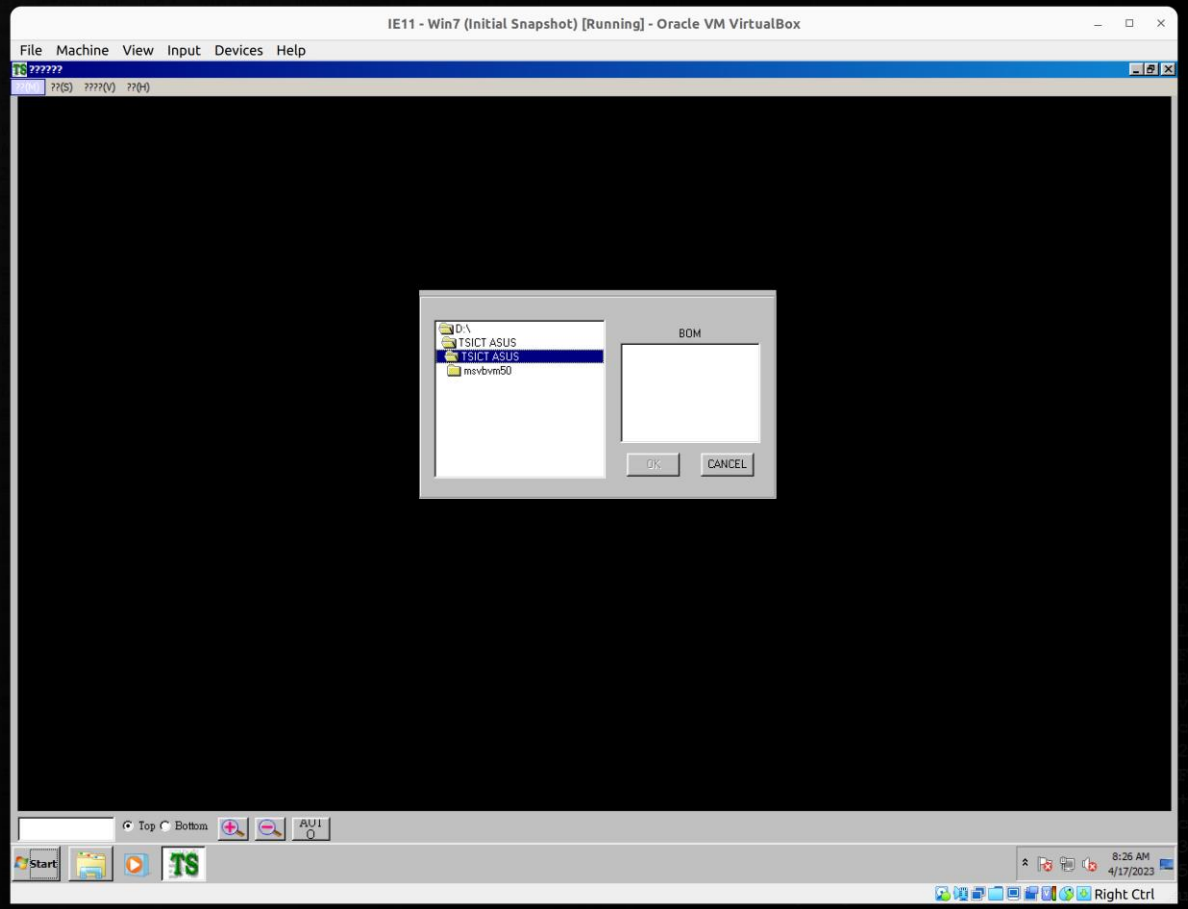
Board View Data



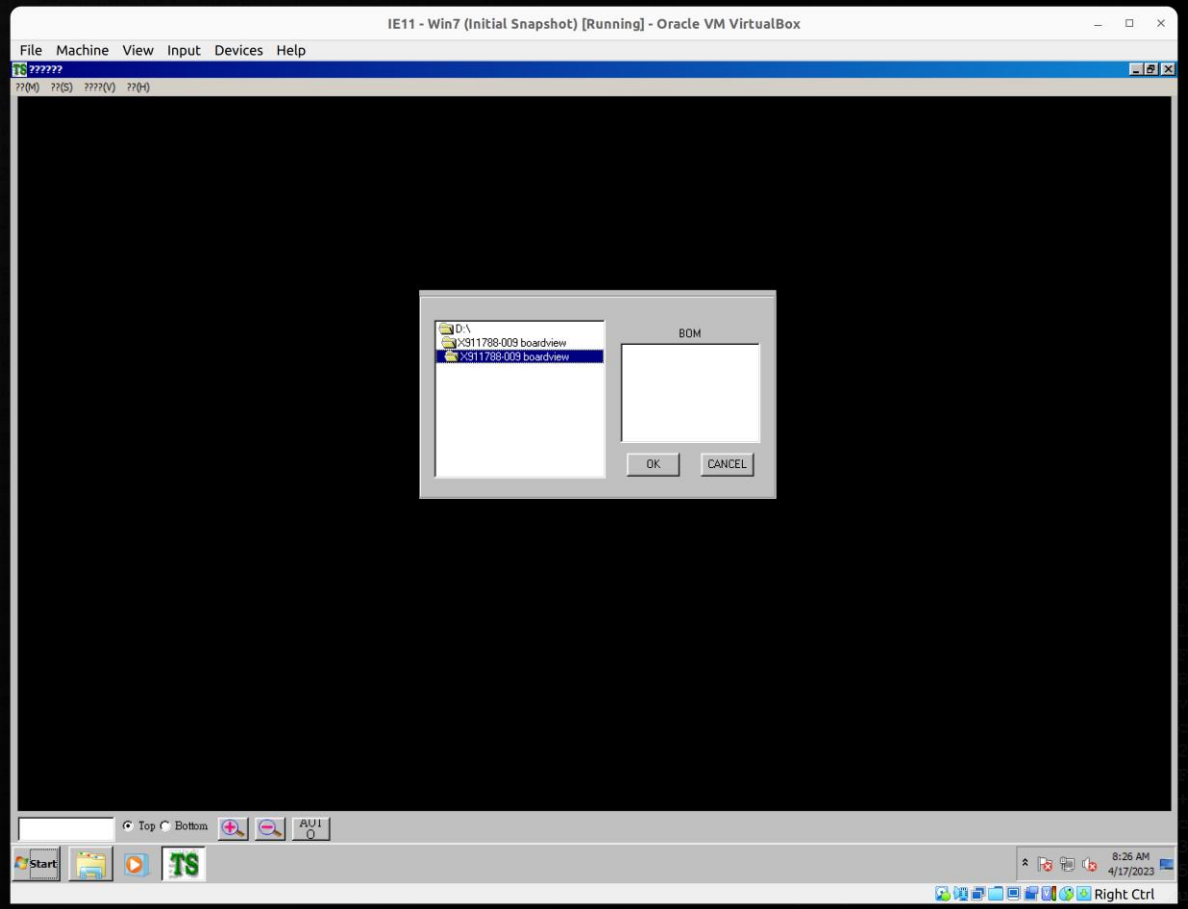
Board View Data



Board View Data

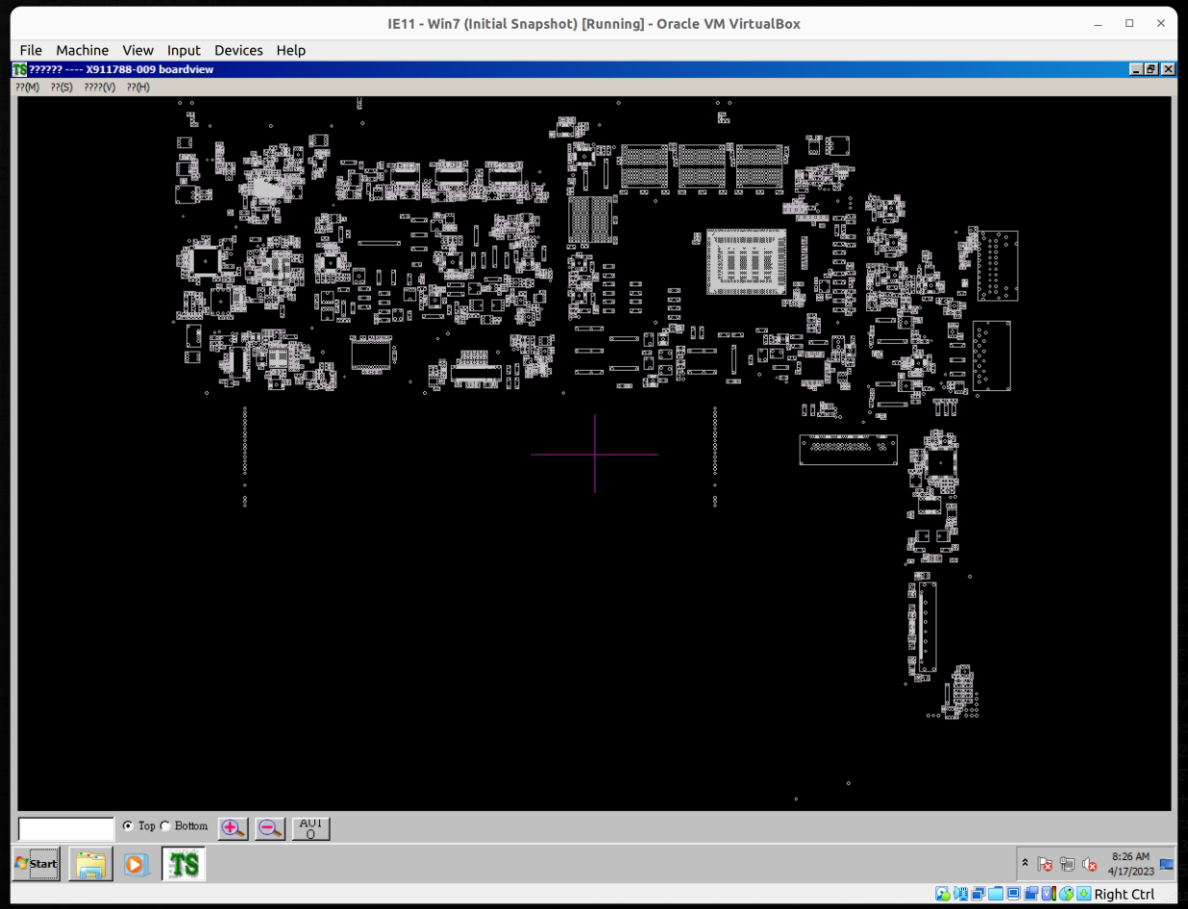


Board View Data



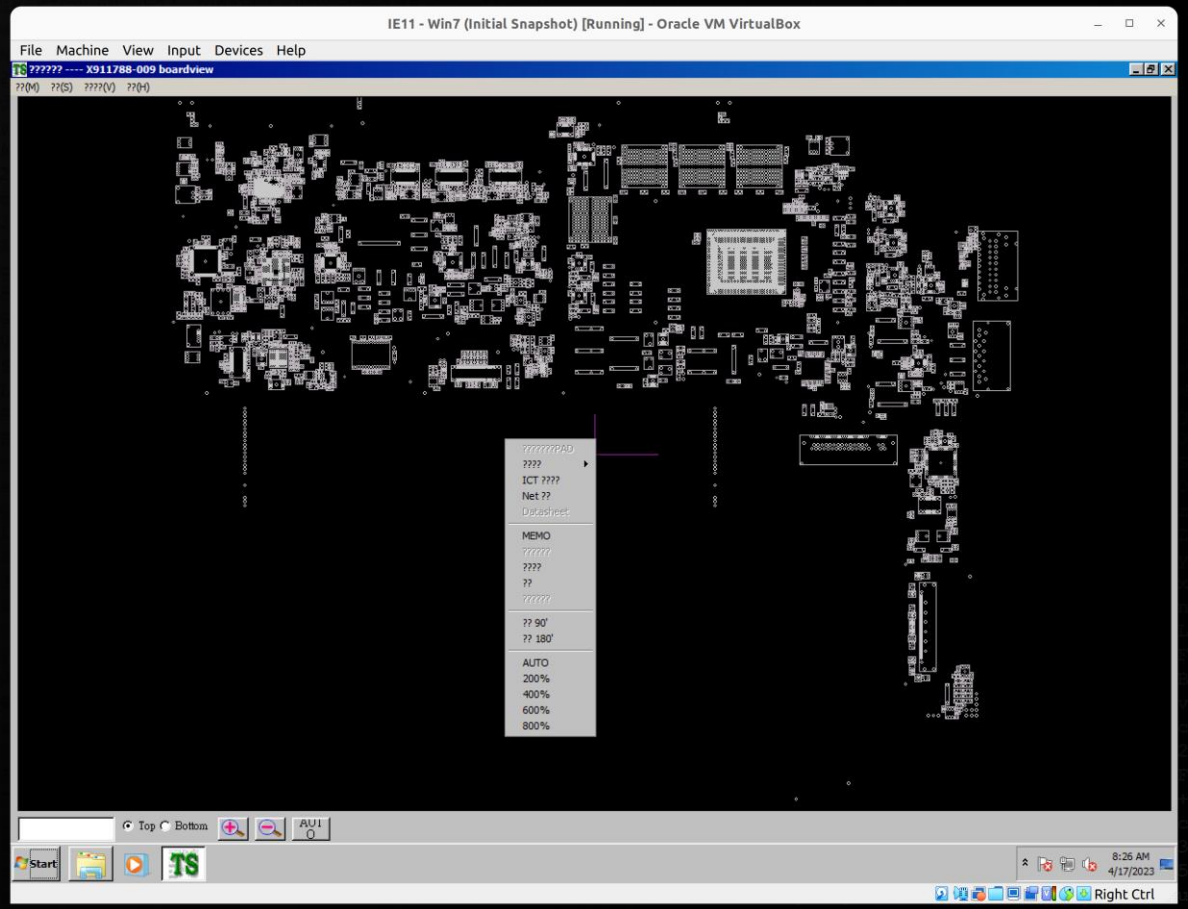
black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Board View Data

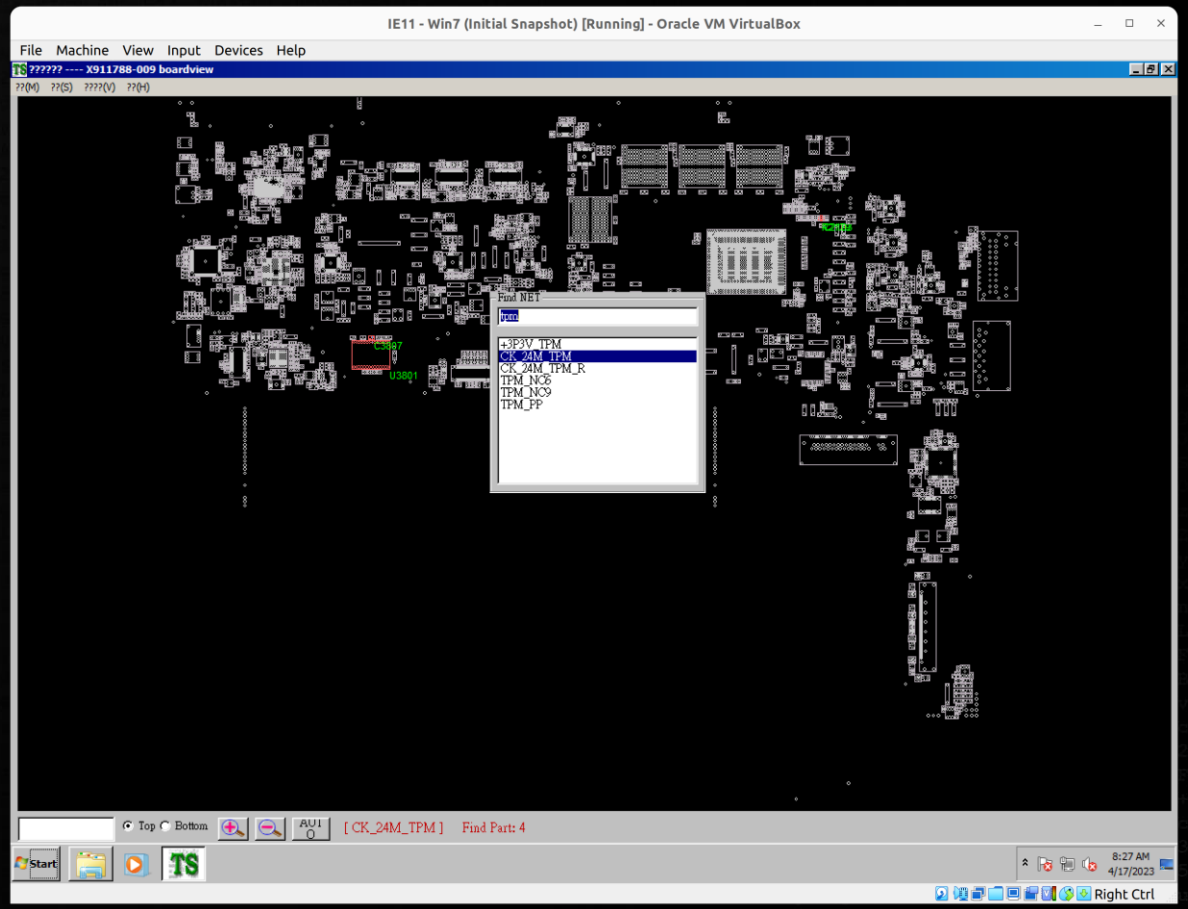


black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Board View Data

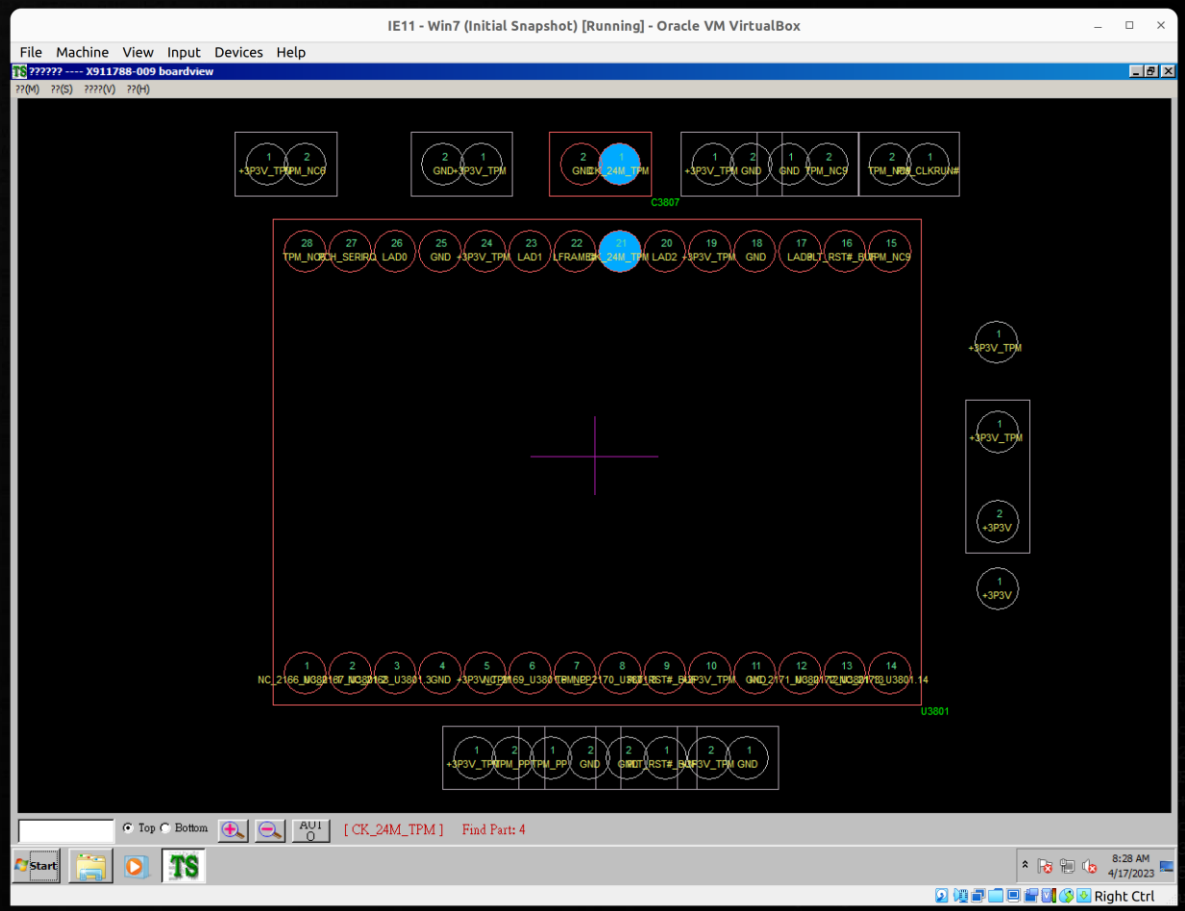


Board View Data



black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Board View Data



Agenda Day 1

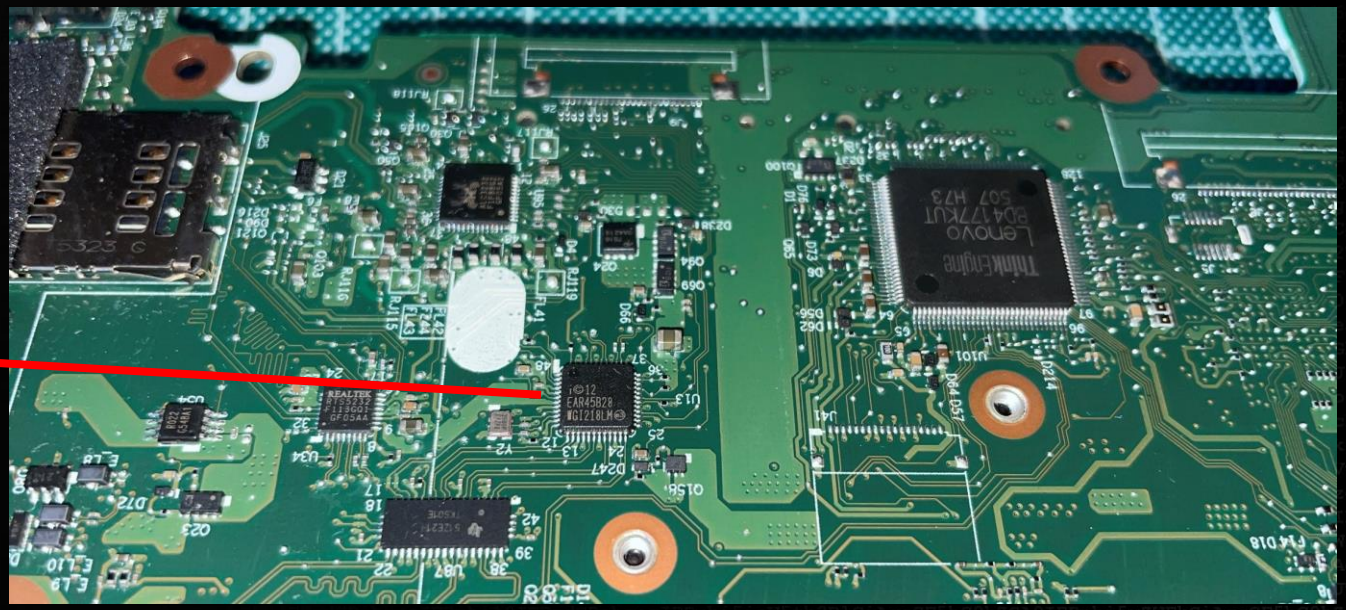
- Equipment Inspection
- Soldering Theory & Lab
- Tamper Protection Switches
- Forensic Data Acquisition
- Notebook Internals
  - Notebook Disassembly

Key Takeaways

- Ability to Solder
- Tamper Protection Switches
- Basic Forensic Data Acquisition

Mainboard Components Practice

- Identify the Chip‘s
  - Check the Chip-ID
  - Ask Google



WGI219V

Intel® Ethernet Connection I218

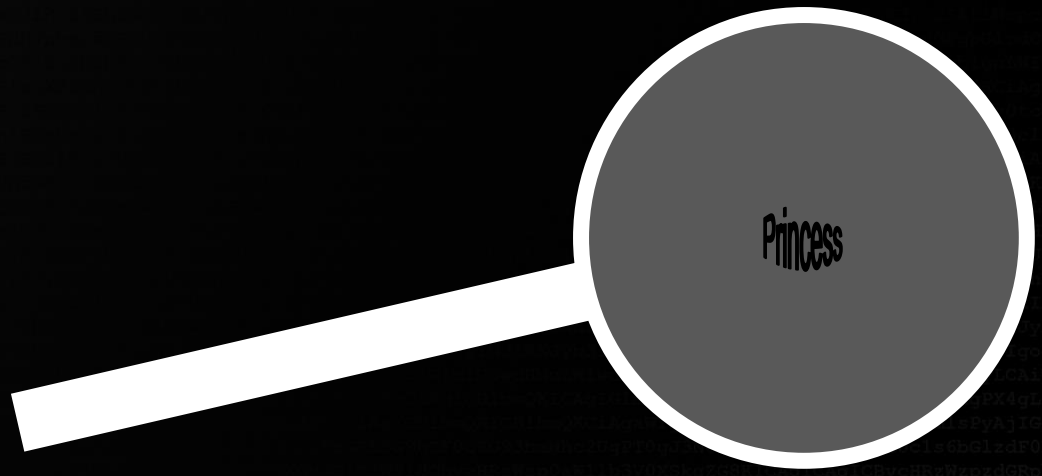
Mainboard Components Practice

- If there is some flux or thermally conductive paste on the Chip
  - Use cleaning agent
  - Use Isopropanol
  - (Sprit)
- If you still can’t read the label on the chip
  - Use your Cellphone with the flash -> take the photo from the side
  - Magnifier
  - Microscope
- Search for the USB, Network, Sound, Graphic, PCI controllers
- Compare findings with other students

Component Identification

- Not only search for the TPM, gather knowledge about your system
- E.g. USB, Network, Sound, Graphic, PCI, SPI, … controllers

- Search in Progress …..



Agenda Day 1

- Equipment Inspection
- Soldering Theory & Lab
- Tamper Protection Switches
- Forensic Data Acquisition
- Notebook Internals
- Notebook Disassembly

Key Takeaways

- Ability to Solder
- Tamper Protection Switches
- Basic Forensic Data Acquisition

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

End of Day 1

- Questions?

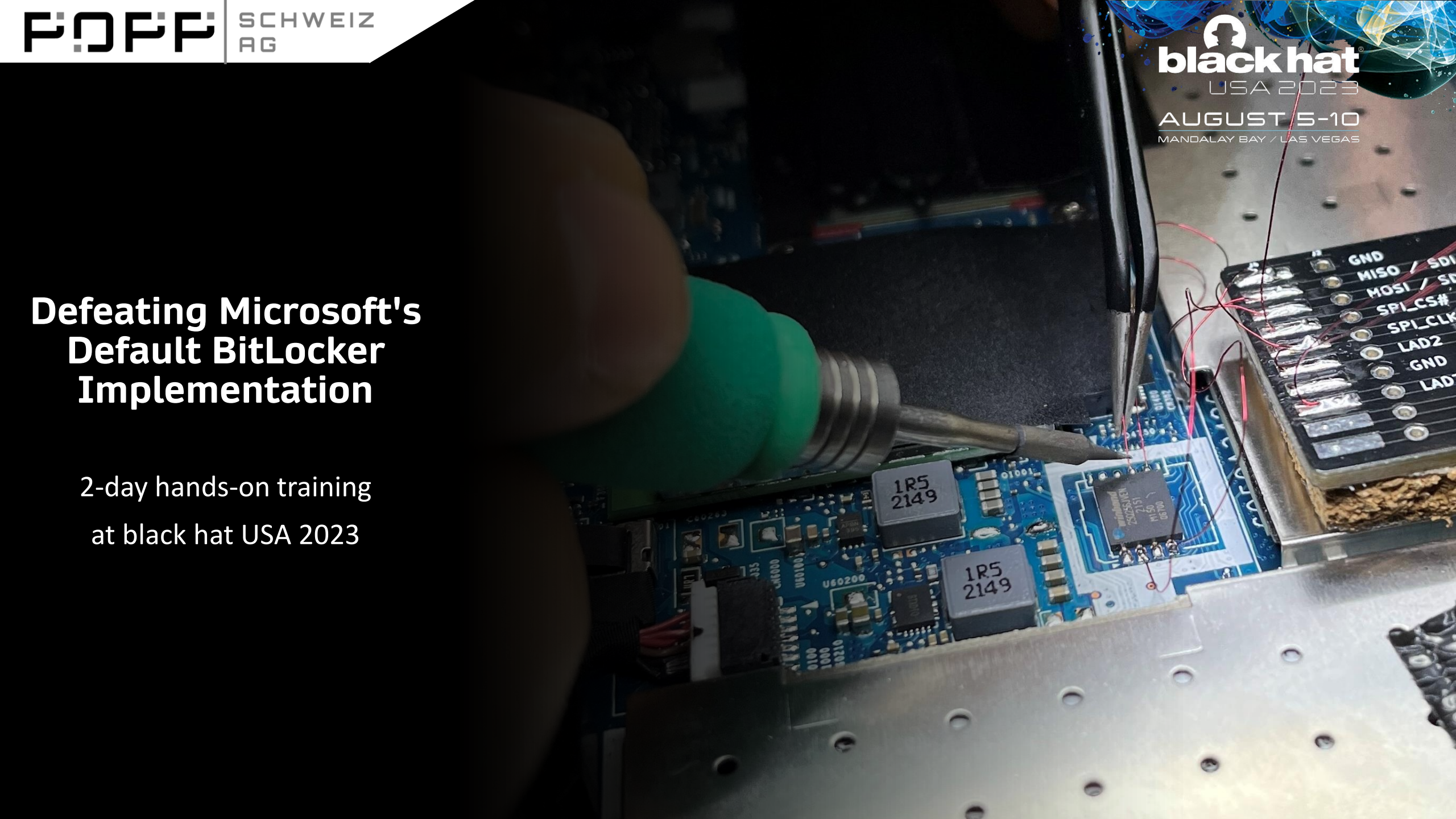
Agenda Day 2

- BitLocker Theory
- TPM Theory
- Soldering to the TPM Bus
- Logic Analyzers & Labs
- Sniffing the Key
- Recovering the Recovery PW
- Extracting Artifacts

Key Takeaways

- BitLocker & TPM Theory
- Logic Analyzers
- Obtaining the Recovery PW

FOFP SCHWEIZ AG



Defeating Microsoft's Default BitLocker Implementation

2-day hands-on training

at black hat USA 2023