



Forensic Locksmithing

HES 2015

Alexandre TRIFFAULT @FrenchKey_fr

alexandre@ouverturefine.com

www.frenchkey.fr

www.serrurerieforensique.fr

Who ?

Alexandre Triffault

- My hobbies :
 - Collecting Locks, Tools and Opening techniques
 - RF and RFID R&D
- My Company : OFC
(Outillage Formation Conseil)
www.ouverture-fine.com
- Websites I run :
 - www.frenchkey.fr
 - www.serrurerieforensique.fr
 - www.locksport.fr



Introduction

- Why physical security matters ?
- Why would anyone use NDE techniques ?



Plan

- How a key works
- NDE techniques and how they act
- Forensic analysis of such techniques
- Anti-forensic
- Countermeasures

How a key works



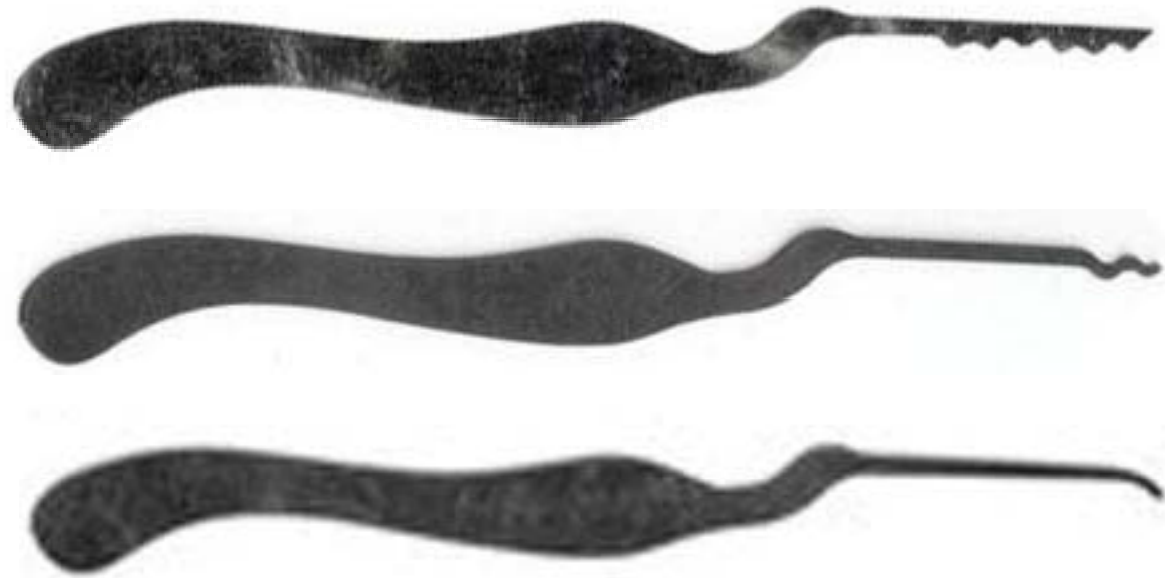
How a key works



NDE techniques and how they act



Basic Lockpicking



Bumping



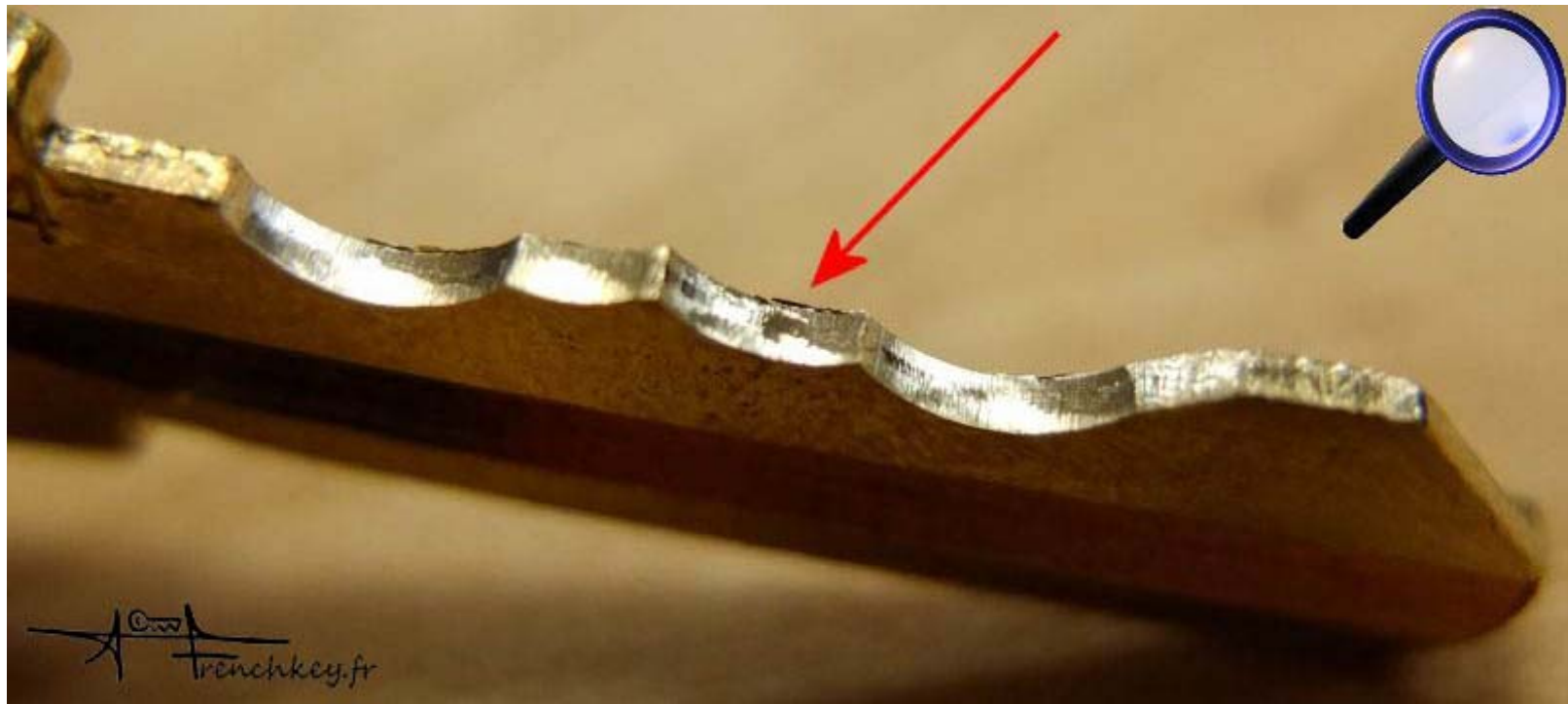
Mechanical pick-gun



Electro pick-gun



Impressioning



video

Forensic Analysis



Forensic Analysis

- Know the target



Forensic Analysis

- Know the target
 - Forums :
 - Locksport.fr
 - Lockpicking101.com
 - Books :
 - Locks Safes and Security
 - High Security Mechanical Locks

Practical Forensic Analysis





Anti Forensic Techniques

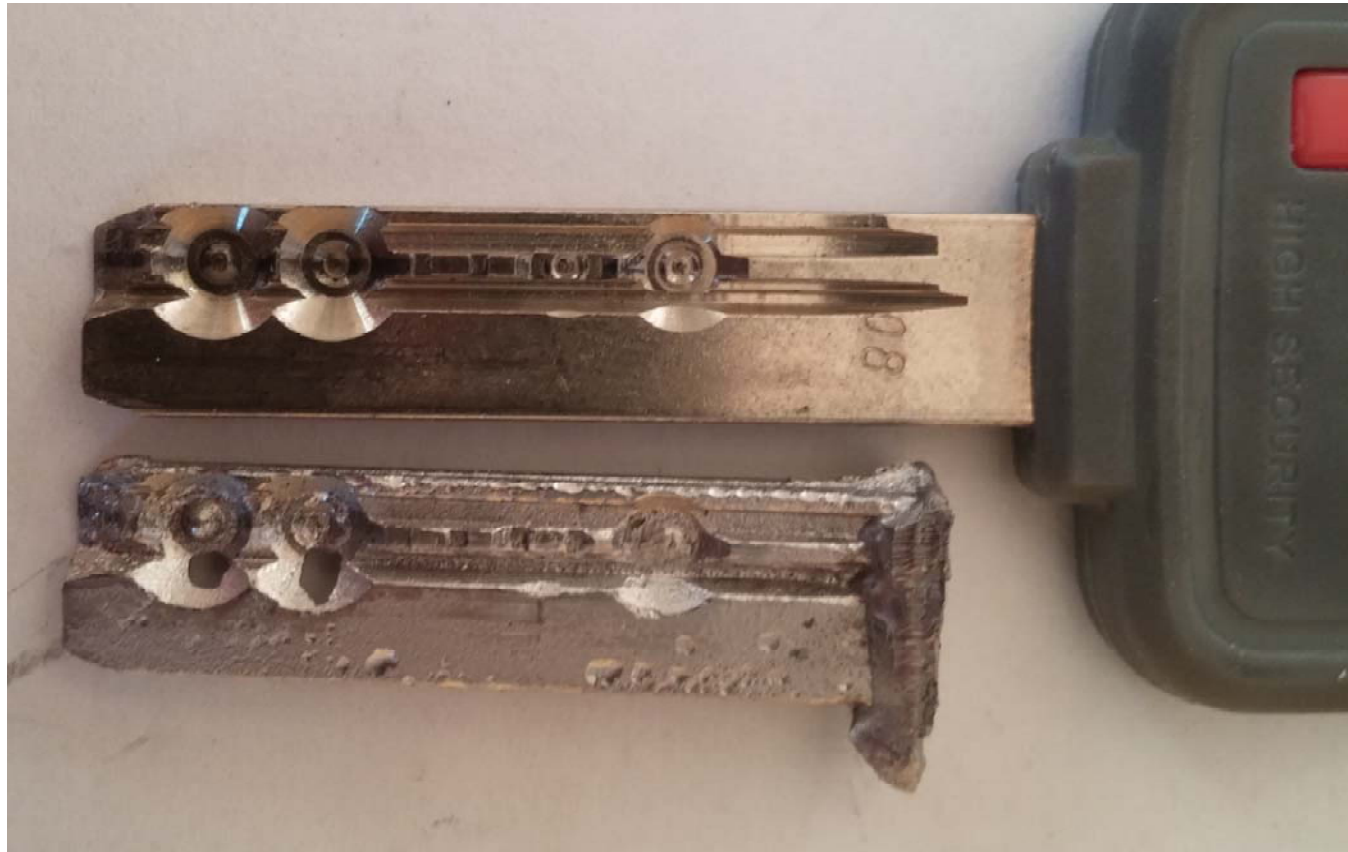
- Key duplication
- Lock decoding
- Lock recoding

Key duplication with trade machines



video

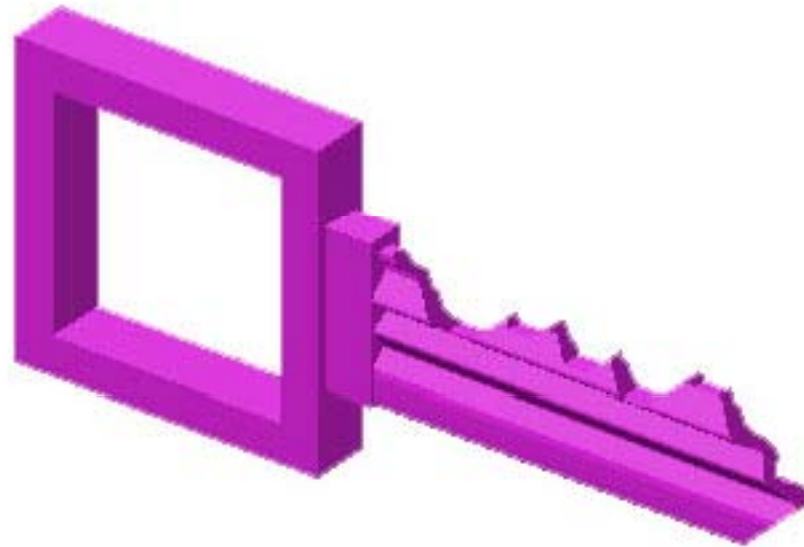
Key duplication by Molding



Key duplication by hand



Key duplication with 3D printing



Lock decoding

- Key duplicating from a picture
- Soft manipulation (Safe locks mostly)
- X-Rays, IR and Doppler attacks
- Right amplification in a Masterkeyed system

Lock recoding

- Very basic attack :
 - Break the lock
 - Take it apart
 - Build a new one with the same combination
 - (and make a working key in the meantime)
- It leaves no regular forensic clue, which is a clue by itself somehow

Countermeasures

- Key duplication can leave traces too



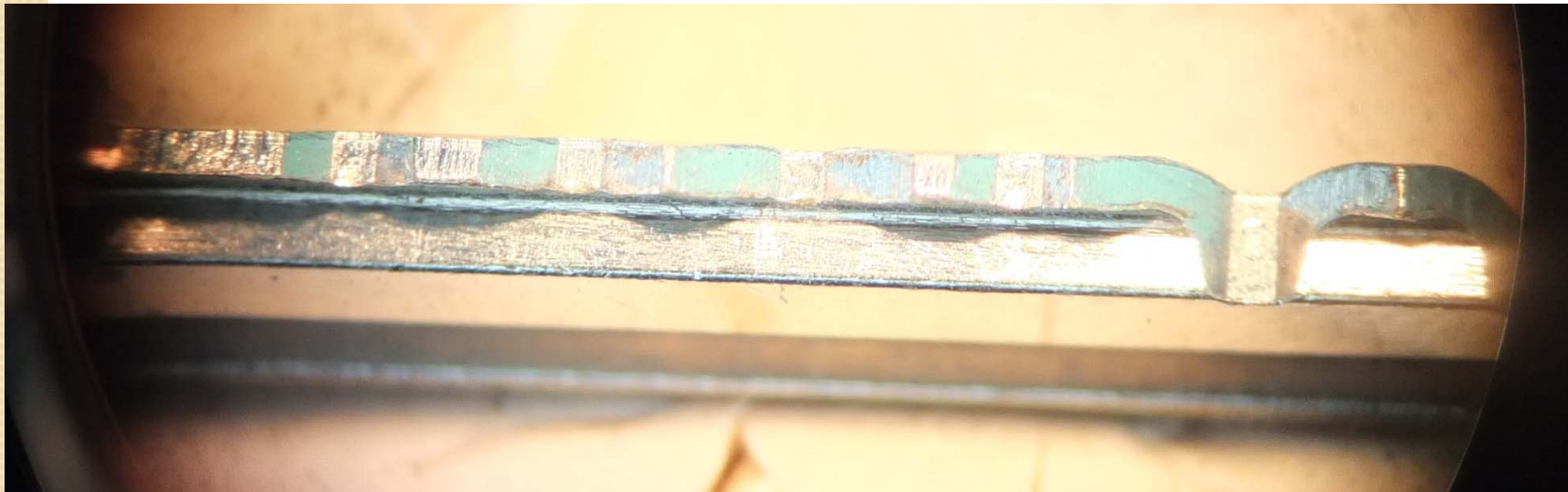
Countermeasures

- Key duplication can leave traces too



Countermeasures

- Key duplication can leave traces too





Countermeasures

- Use hard to duplicate/replicate keys
- Know your material and its flaws
- Hide your keys !



Conclusion

Do forensic when you have a data leak,
you could find surprising stuff about how
that leak occurred



Questions, suggestions ?

Thank You !

