Forensics, Malware and Penetration Testing

Intro to Forensics

Andreea Radu and David Oswald
University of Birmingham

a.i.radu@bham.ac.uk

Outline

1. Disk forensics
2. Log file forensics

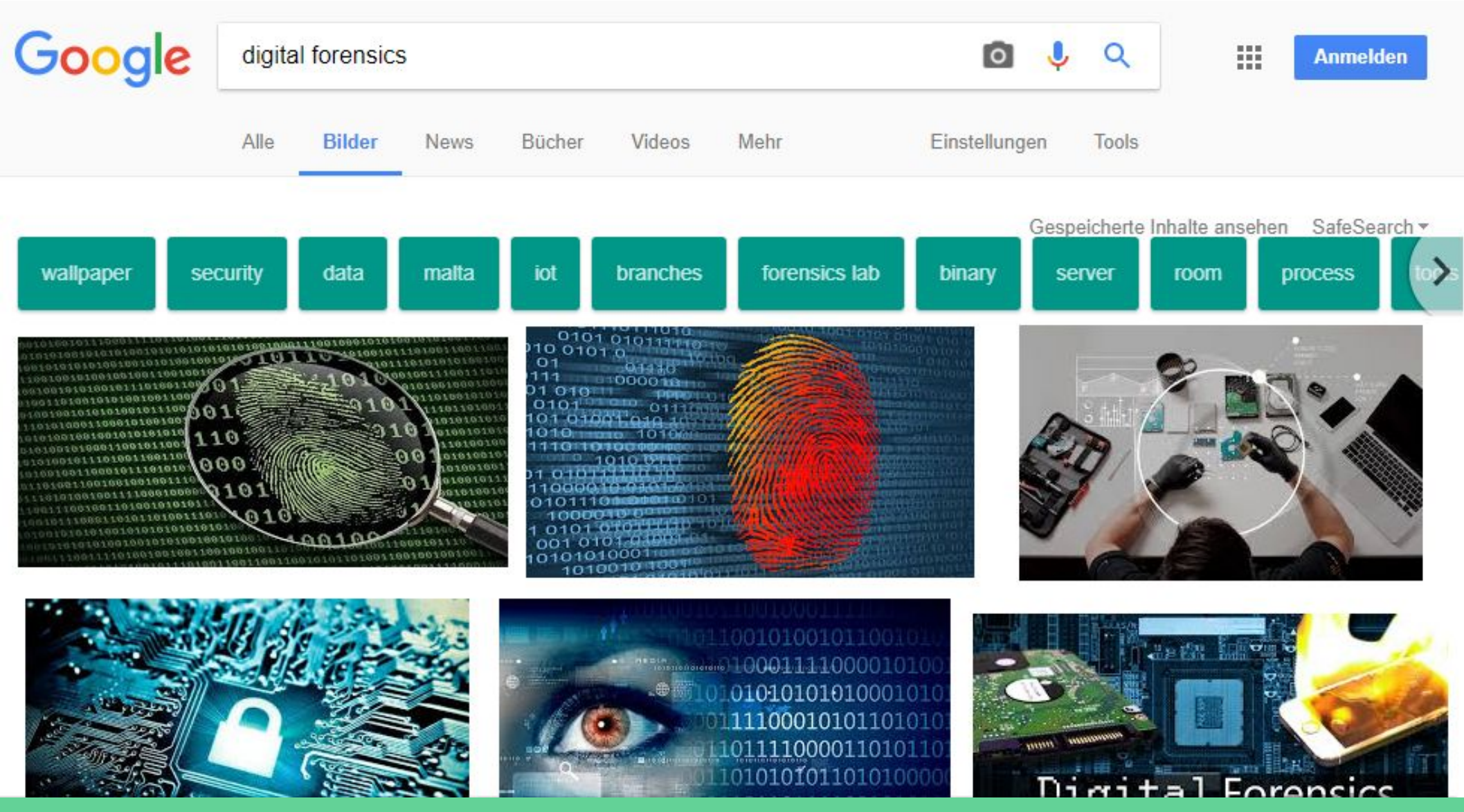
3. Network forensics
4. Memory forensics

5. Mobile devices (Android) ➔ David

Tools

- Mostly Linux command line / GUI
- Little / no programming required
- The Archlinux VM has all the tools – see Canvas for instructions
- Some tools also run fine/better under Windows (esp. Autopsy)
- Most tools can also run under other Linux distros, using VMs is often easier though

Why Digital Forensics?



Example 1: Dealing with a security incident

KASPERSKY lab

INITIAL ATTACK

The initial attack against Kaspersky Lab began with the targeting of an employee in one of our smaller APAC offices. The original infection vector for Duqu 2.0 is currently unknown, although we suspect spear-phishing e-mails played an important role. This is because for one of the patients zero we identified had their mailbox and web browser history wiped to hide traces of the attack. Since the respective machines were fully patched, we believe a zero-day exploit was used.

In 2011, we were able to identify Duqu attacks that used Word Documents containing an exploit for a zero-day vulnerability (CVE-2011-3402) that relied on a malicious embedded TTF (True Type Font File). This exploit allowed the attackers to jump directly into Kernel mode from a Word Document, a very powerful, extremely rare, technique. A similar technique and zero-day exploit ([4]CVE-2014-4148) appeared again in June 2014, as part of an attack against a prominent international organization. The C&C server used in this 2014 attack as well as other factors have certain similarities with Duqu, however, the malware is different from both Duqu and Duqu 2.0. It is possible that this is a parallel project from the Duqu group and the same zero-day (CVE-2014-4148) might have been used to install Duqu 2.0.

Example 2: Police investigations

http://www.ntnews.com.au/news/northern-territory/northern-territory-police-fraud-squad-seize-computers-and-documentation-from-darwin-travel-agency/story-fnk0b1zt-1227171355287

German cyber-attack: man admits massive data breach, say police

A 20-year-old man has admitted to police that he was behind one of the country's biggest data breaches, in which the private details of almost 1,000 public figures were leaked.

The man, who lives with his parents in the central German state of Hesse and is still in the education system, told police he had acted alone and was not politically motivated.

He told investigators he had been driven instead by his annoyance at statements made by the victims of his attacks, including politicians, journalists and leading celebrities.

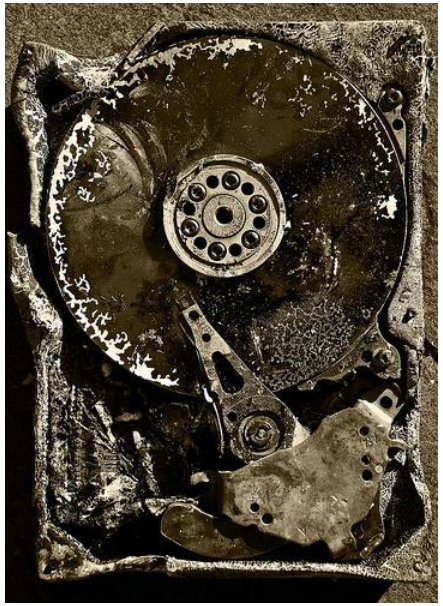
The hacker, who used the pseudonyms "G0t" and "Orbit", was arrested on Sunday after investigators searched his home. On Monday, he confessed to the cyber-attack, prosecutors said. He is accused of spying, leaking data and the unwarranted publication of personal data.

Investigators traced the man through digital tracks he left on the internet, as well as by speaking to witnesses, including a 19-year-old man with whom the hacker had communicated via an encrypted messaging service. The hacker told him he had destroyed his computer to avoid detection, but police said they had recovered extensive evidence.

https://www.theguardian.com/world/2019/jan/08/germany-data-breach-man-held-in-suspected-hacking-case

Other examples and related areas

- Data recovery from damaged systems
- Understanding hardware and software faults
- Penetration testing (e.g. OS security)



Digital Forensics: Standards & Guidelines

(The boring part ...)

Digital Forensics in the UK

- ACPO: “Good Practice Guide for Digital Evidence“
  (ACPO = Association of Chief Police Officers)
- Mostly oriented towards law enforcement
- Collection of best practices, not necessarily legally binding

ACPO Guide & Principles

Four principles are involved:

Principle 1:

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3:

An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

NIST SP 800-86

PCI PFI Program Guide

Appendix A: Forensic Investigation Guidelines

In accordance with applicable Industry Rules, a Compromised Entity that stores, processes, or transmits payment card data and is the subject of a Security Issue must ensure that only a PCI Forensic Investigator approved under the PCI SSC PFI Program is engaged to perform a forensic investigation thereof. All PFIs are required to adhere to the following forensic investigation guidelines in all PFI Investigations. Compromised Entities can also use these guidelines to monitor the work of the PFI.

PFI Investigations must be conducted using the following scope and methodology:

1. The PFI will determine the scope of the forensic investigation and relevant sources of electronic evidence. This includes, but is not limited to:
    - Assessment of all external and internal connectivity points within each location involved.
    - Assessment of network access controls between compromised system(s) and adjacent and surrounding networks.
2. The PFI will acquire electronic evidence from toe C mpromised Entity's h st and network-based systems.

https://www.pcisecuritystandards.org/documents/PFI_Program_Guide_2.1.pdf

Next part: Disk Forensics