HERIOT WATT UNIVERSITY

Topic 1: Intro to digital forensics

F20FO/F21FO – Digital Forensics

Mike Just (Edinburgh)
Ryad Soobhany (Dubai)

LEADERS IN IDEAS AND SOLUTIONS

Topic overview

- Topic 1 overview: Introduction to digital forensics
  - Computer security
  - Computer crimes
  - Digital evidence & forensics

Learning Outcomes

- Demonstrate understanding of computer security and crime related to digital forensics
- Define and understand concepts in digital forensics
- Appreciate importance of digital evidence to digital forensics

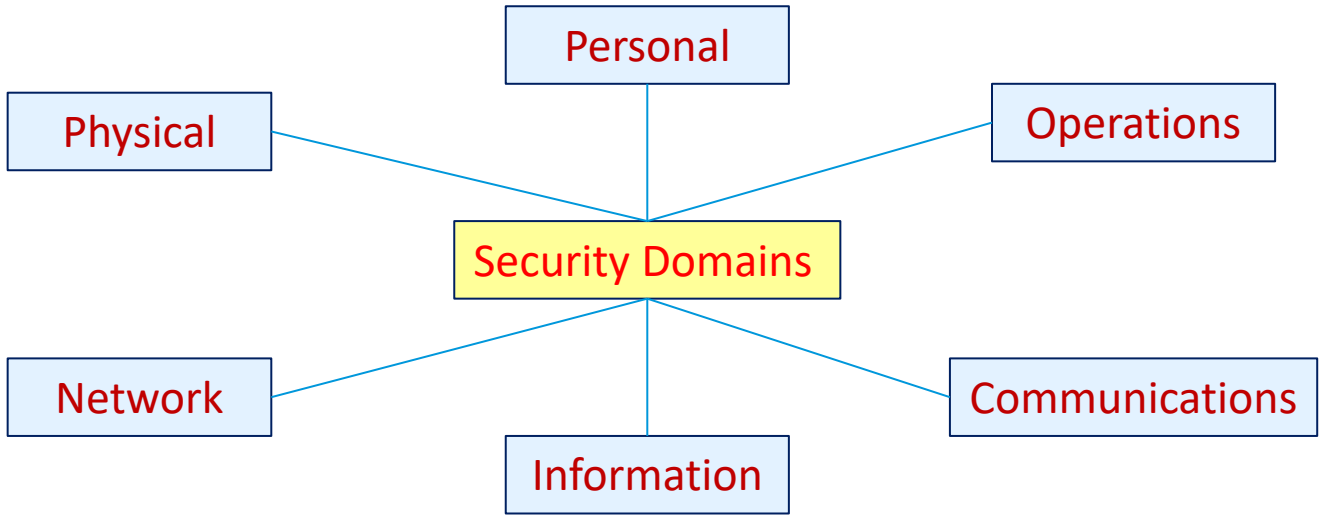
HERIOT WATT UNIVERSITY

LEADERS IN IDEAS AND SOLUTIONS

Computer Security

What is Security

- "The quality or state of being secure—to be free from danger"
- A successful organisation should have multiple layers of security in place – but what is the weakest link?



What is Security

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools:
  - policy,
  - awareness,
  - training,
  - education,
  - technology

What is Security

- Users
  - Can perform only the tasks they are authorised to perform
  - Can obtain only the information that they are authorised to obtain
  - Cannot cause damage to the data, application software, or operating environment of a system
- Assuring that data access is available on an uninterrupted basis

Goals of Computer Security

- **Confidentiality**
  - Prevent the disclosure of sensitive information from unauthorised people resources, and processes
- **Integrity**
  - The protection of system information or processes from intentional or accidental modification
- **Availability**
  - The assurance that systems and data are accessible by authorized users when needed

Goals of Computer Security

- **Other goals** of computer security
  - Authentication, Access control and Authorisation (and Anonymity)
  - Accountability
    - Maintenance of logs, back-ups
    - Support for non-repudiation

Computer security "vs" digital forensics

- **Computer security**: protecting resources
- **Digital forensics:** what happened (or is happening) based on computer-related (digital) evidence related to a suspected crime
  - Some overlap with accountability goal of computer security
- CS & DF collaborate, e.g., incident management

Achieving the computer security goals is primarily covered in other courses (computer network security, advanced network security)

HERIOT WATT UNIVERSITY

LEADERS IN IDEAS AND SOLUTIONS

Computer Crime

Crimes Happen

Low tech crime	High tech crime
Smash & Grab robbery Brick, crowbar, mask, bag	Bank Account robbery Computer, network access

Need to collect evidence after (and sometimes during) a crime

Example of High Tech Crime

Why do we care?

Nearly 157,000 had data breached in TalkTalk cyber-attack

Company says over 15,000 also had financial details hacked but most codes obtained could not be used for payments

Cyber Attack Targets Britain's HSBC Bank

HSBC said it had successfully repelled a DDoS attack on Jan. 29, although online access to banking services was disrupted.

"Lockdroid" Ransomware Can Lock Smartphones, Erase Data

A new piece of Android ransomware has emerged, capable of locking devices, changing PINs, and even fully wiping user data via factory resets, Symantec researchers warn. [Read More]

Ukrainian blackout caused by hackers that attacked media company, researchers say

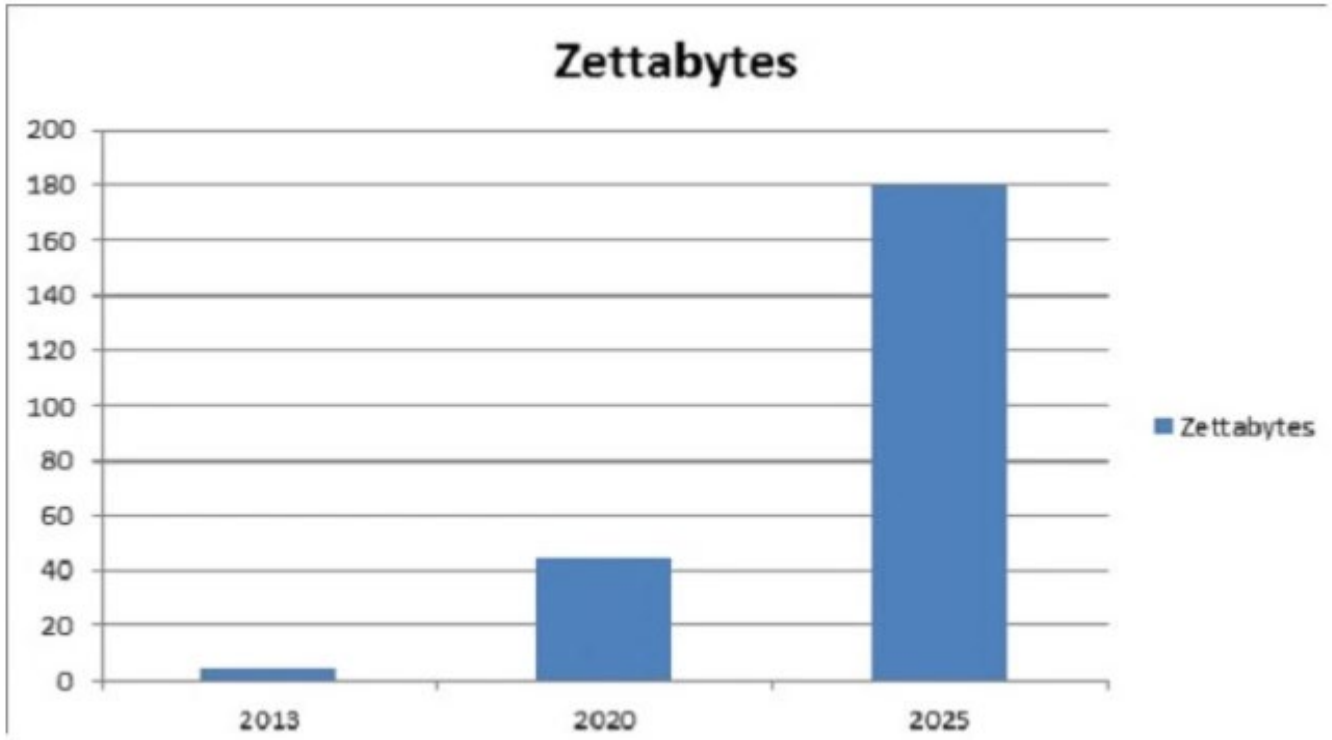
Cybersecurity experts 'charge £10,000 a day to protect UK's top firms'

Data has value

By 2025,

- more than 20 billion devices connect to the Internet
- 152,000 devices connect to a network a minute

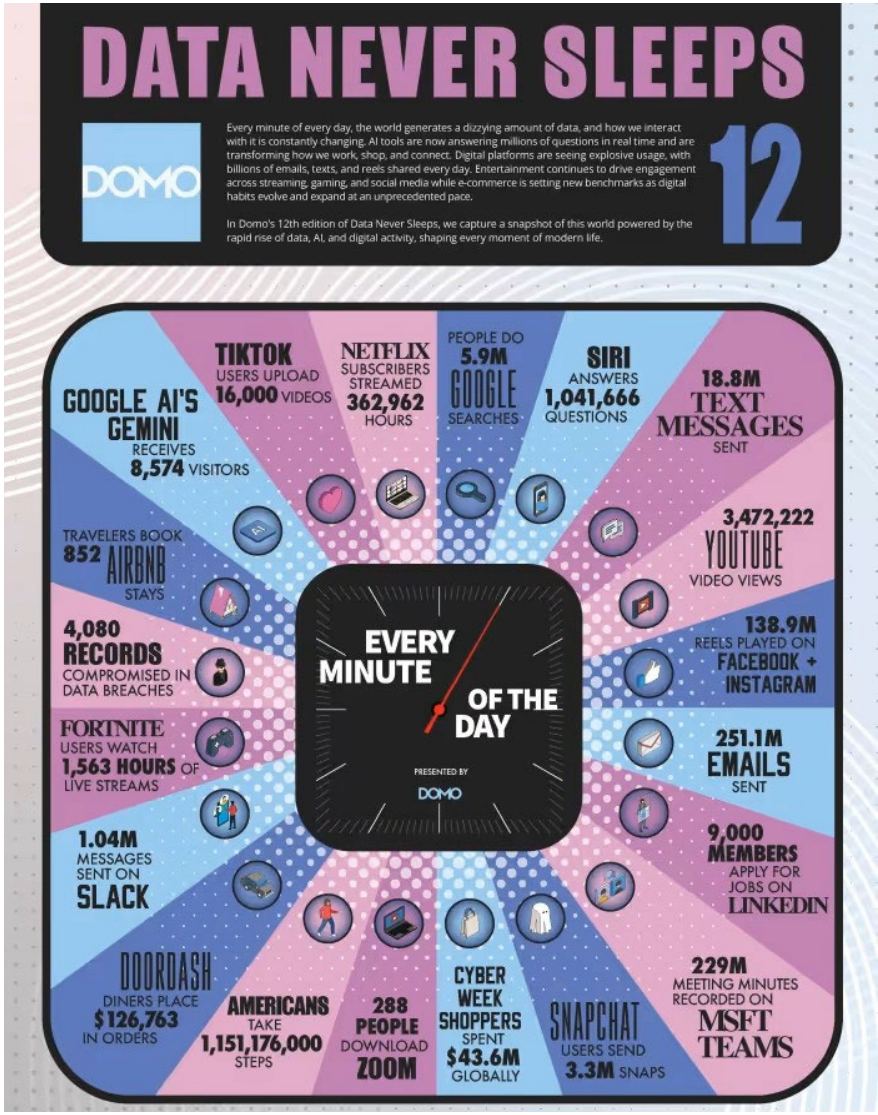
- 1000 **kilobytes** = 1 Megabyte
- 1000 **Megabytes** = 1 Gigabyte
- 1000 **Gigabytes** = 1 Terabyte
- 1000 **Terabytes** = 1 Petabyte
- 1000 **Petabytes** = 1 Exabyte
- 1000 **Exabytes** = 1 Zettabyte
- 1000 **Zettabytes** = 1 Yottabyte
- 1000 **Yottabytes** = 1 Bronobyte
- 1000 **Bronobytes** = 1 Geopbyte



https://iot-analytics.com/number-connected-iot-devices/

How Much Data Generated

- Data generated on the internet every minute across popular applications and platforms
- Instagram, TikTok, Amazon, WhatsApp, Netflix, etc.



https://www.domo.com/learn/infographic/data-never-sleeps-12

Devices and Data

Data is valuable

Sentimental Data

Social Media

Financial Details

Mobile Devices

Official ID card

Work Credentials

What valuable data do you hold?

- Financial details
  - Bank account
- Your ID
  - Passport or ID card (e.g. Emirates ID)
- Phones and Laptops
  - Messages
  - Photos
  - Social media


WIFI
BTBUSINESSHub-902
Password: 0049177808

Example 1: Southern Water

https://www.sharp.co.uk/news-and-events/blog/the-biggest-uk-cyber-attacks-of-2024

Company: Southern Water

Month of cyber attack: February | **Industry:** Essential Services

What happened?

On 12 February 2024, Southern Water announced that data from a limited part of their server estate had been stolen following an illegal intrusion into their IT systems. This incident was discovered during an ongoing investigation into suspicious activity.

Who was affected?

Southern Water's operations and services to customers were not affected by the cyber attack but a data breach did occur.

The breach affected some of Southern Water's customers, as well as current and former employees. Approximately 5-10% of their customer base was notified that their personal data might have been impacted.

Example 2: JLR

Jaguar Land Rover supply chain attack

Date: August 2025

Attack type: Ransomware and supply chain disruption

Threat actor: Scattered Lapsus$ Hunters

In August 2025, Jaguar Land Rover suffered what is widely regarded as the most economically damaging cyber incident in UK history. According to the Cyber Monitoring Centre, the attack is expected to cost £1.9 billion and brought production to a halt for five weeks. More than 5,000 businesses across JLR's global supply chain were affected, with full recovery not expected until January 2026.

The attack was attributed to the Scattered Lapsus$ Hunters, a loosely affiliated collective linked to groups such as Lapsus$, Scattered Spider, and ShinyHunters. By exploiting vulnerabilities in third-party supplier software, the attackers were able to move laterally into JLR's core systems. Ransomware crippled production and logistics networks, forcing temporary shutdowns at manufacturing sites in the UK, Slovakia, and Brazil.

Beyond operational disruption, the attackers threatened to leak sensitive design and supplier data unless multimillion-pound ransom demands were met.

https://insights.integrity360.com/the-biggest-cyber-attacks-of-2025-and-what-they-mean-for-2026

Example 3: NHS

News

Synnovis cyber attack – statement from NHS England

21 June 2024

Digital

On 3 June, Synnovis, a pathology laboratory which processes blo number of NHS organisations, primarily in South East London, w cyber attack.

https://www.sharp.co.uk/news-and-events/blog/the-biggest-uk-cyber-attacks-of-2024

Company: NHS

Month of cyber attack: June | **Industry:** Healthcare

What happened?

On 3 June 2024, Synnovis, a pathology laboratory that processes blood tests for several NHS organisations, primarily in South East London, was targeted by a ransomware attack. The attack was carried out by a cyber criminal group who claimed to have stolen and published sensitive data from Synnovis' systems.

Who was affected?

The breach potentially impacted patients whose blood tests were processed by Synnovis. The stolen data included sensitive patient information, although the full extent of the data compromised is still under investigation. The attack caused significant disruption to blood testing services in South East London, leading to delays and rescheduling of some medical appointments.

Example 4: CrowdStrike

Microsoft | Official Microsoft Blog Our Company News and Stories

Helping our customers through the Cro outage

Jul 20, 2024 | David Weston - Vice President, Enterprise and OS Security

On July 18, CrowdStrike, an independent cybersecurity company, released a software impacting IT systems globally. Although this was not a Microsoft incident, given it im we want to provide an update on the steps we've taken with CrowdStrike and others support our customers.

https://www.sharp.co.uk/news-and-events/blog/the-biggest-uk-cyber-attacks-of-2024

Company: CrowdStrike

Month of cyber attack: July | **Industry:** Technology

What happened?

On 19 July 2024, CrowdStrike, a cyber security company, released a faulty update to its Falcon Sensor security software.

This update caused widespread issues with Microsoft Windows computers running the software, leading to a massive IT outage.

Who was affected?

The outage had a broad impact, approximately 8.5 million Windows devices worldwide experienced crashes and were unable to restart properly. Airlines, hospitals, banks, and governmental services experienced significant disruptions to their services.

For example, UK GP services lost access to patients test results and appointment information, causing major disruption to services.

Although it has not been quantified yet, the financial damage from this incident is estimated to run into the billions.

Example 5: TfL

TfL provides update on ongoing cyber security incident - 12 September

12 September 2024

TfL today (Thursday 12 September) issued an update in relation to the c
incident that it is managing.

https://www.sharp.co.uk/news-and-events/blog/the-biggest-uk-cyber-attacks-of-2024

Company: Transport For London (TfL)

Month of cyber attack: September | **Industry:** Transport

What happened?

On 1 September 2024, Transport for London (TfL) detected suspicious activity on their IT systems. This led to the discovery of a significant cyber attack that involved unauthorised access to customer and staff data.

Immediate action was taken by TfL and an investigation was launched in collaboration with the National Crime Agency and the National Cyber Security Centre.

Who was affected?

TFL have announced that nearly 5,000 customers have been impacted by the data breach, confirming that customer names and contact details were accessed. With the possibility that bank account numbers, sort codes and Oyster card refund data may have also been accessed.

Letters have been posted to these customers detailing the attack, but despite the breach, the physical TfL transport services have been unaffected by this cyber attack.

What steps you take to secure Data

- Use of strong passwords, pincodes
- Encrypt data
- Use anti-virus, firewall
- Use a physical lock
- Back-up data
- Secure channels when working remotely

The above (and other security) techniques:

- Help to provide computer security
- Can both help (e.g., back-up data) and hinder (e.g., encrypted data) the collection of DF evidence

Large-Scale Approaches to Crime Reduction

NCA and FBI Lead LockBit Takedown with Operation Cronos

Read the story here

The UK's NCA teamed up with
infrastructure used by LockBit
service (RaaS) group worldwid

Two Operations Take Down Botnets and Ransomware Operations on the Same Day

Read the 911 S5 takedown story here and Operation Endgame story here

The end of May 2024 was hectic for law enforcement worldwide. In the US, the Department of Justice (DoJ) announced on May 29 the takedown of 911 S5 Botnet, a global network of millions of compromised residential Windows computers used to facilitate cyber-attacks, large-scale fraud, child exploitation and other serious criminal activity.

Police Swoop on Black Axe Cybercrime Syndicate in Operation Jackall III

Read the story here

On July 17, Interpol said it had struck a significant blow against several West African cybercrime groups, including the notorious Black Axe syndicate.

https://www.infosecurity-magazine.com/news-features/top-10-cyber-law-enforcement-2024/

HERIOT WATT UNIVERSITY

Digital Evidence & Forensics

LEADERS IN IDEAS AND SOLUTIONS

Computer security and digital forensics

- Computer security aims to protect resources and preserve a system as it is meant to be according to its security policy

- Digital forensics (DF) sets out to explain how the policy may have been violated, a process that may reveal fatal gaps in the policy itself
  - To explain the violation, DF must involve the collection of evidence

Computer security and digital forensics

- Note the different approaches, depending on which "hat" you're wearing
- For when a computer-related crime occurs

1. A computer security practitioner wants to know when the crime succeeded and whether security policy can be improved to prevent future occurrences
2. A digital forensics practitioner wants to know what happened, when, who was involved, …

While there are some differences in goals, there is some overlap as both are concerned with **incident response**

Digital Evidence & Crime

Three types of situations:

- Device used to conduct crime
  - Child pornography/exploitation
  - Threatening letters
  - Fraud, embezzlement
  - Theft of intellectual property
- Device is target of crime
  - Incident response
  - Security breach
- Device is used as part of the crime
  - E.g., a smartphone tracks a suspect's location

Scenario – Car Accident

You attend a Car Accident

- What Physical Evidence can you collect to figure out what happened?
  - Skid marks
  - Witness statements
  - Pictures of scene

Scenario – Car Accident

- What about Digital Evidence?
  - Car ECU (Engine Control Unit)
  - GPS
  - Camera

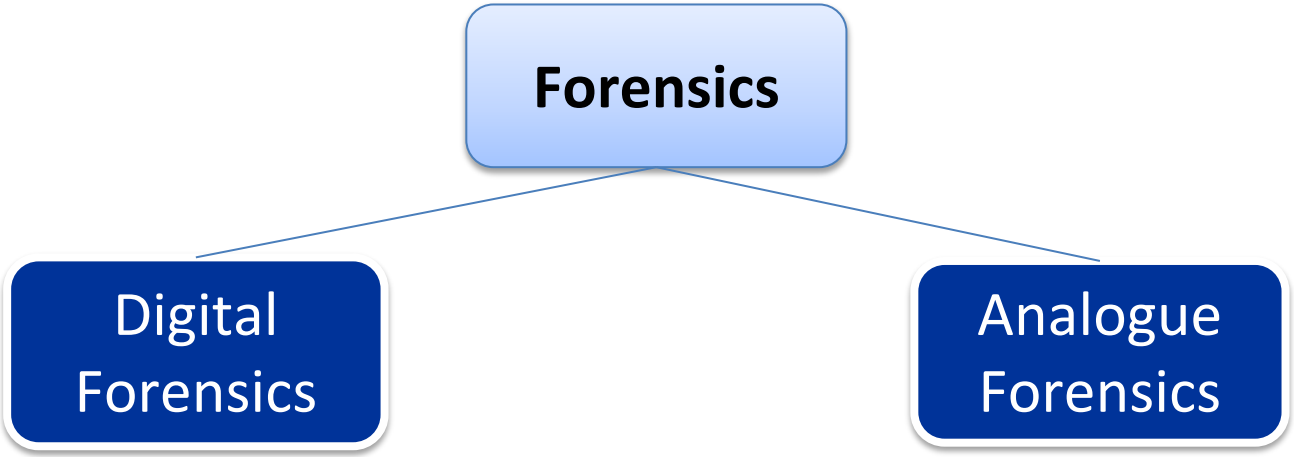
Data challenges for DF

- Deleted data
- Someone else deleted the data
- Computer crashed with unsaved data
- Misplace portable storage
- Data is encrypted

Forensics

The use of scientific methods and technology to solve crimes

– process to the legal system



What is Digital Forensics

Scientific examination of data from digital devices and networks that can be used as evidence

- **Acquisition**
- **Identification**
- **Evaluation**
- **Presentation**

Mix of Computing, Forensic and Legal

What is Digital Forensics

- Procedures are followed, but flexibility is expected and encouraged, because the unusual will be encountered

Digital Evidence

- Data stored or transmitted in digital medium
  - Computer systems
  - Mobile devices
  - Storage
  - Computer network
- Data collection needs to be performed following strict procedures, at least so that it's legally admissible (to ensure objective trust in results)
- Collected data must be done through a chain of custody so that its integrity is maintained from the point of its acquisition

Digital Evidence

Photo by Simon Daoudi on Unsplash

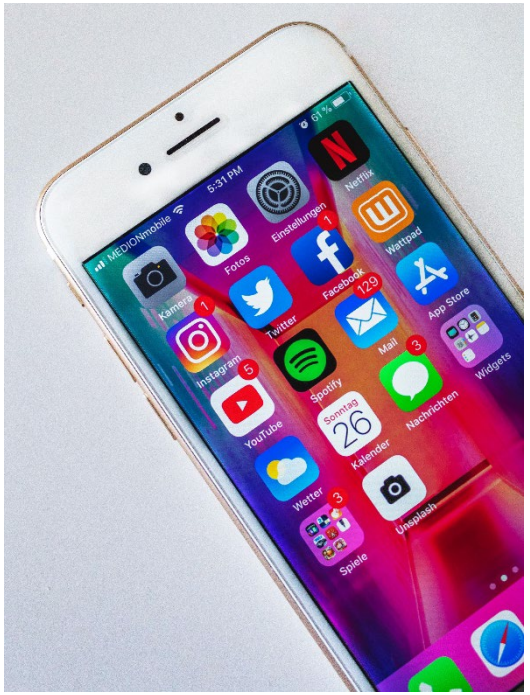


Photo by Sara Kurfeß on Unsplash

Mobile Devices & Crime

- Can have a Direct effect in crime:
  - Instrument of crime
- Can have an Indirect effect
  - hold data such as contacts, SMS, MMS
- Hold valuable data
- 80% of all criminal investigations in Europe involved mobile devices

Digital Forensics in the News

FORBES > INNOVATION > CYBERSECURITY

Digital Forensics Reignites 2019 Cold Case Murder Of Kimberly Bell

Lars Daniel Contributor ⓘ

Lars Daniel covers digital evidence and cybersecurity in life and law.

0

Updated Oct 23, 2024, 01:49pm EDT

FORBES > INNOVATION > CYBERSECURITY

How Digital Forensics Experts Read Your Encrypted WhatsApp Messages

Lars Daniel Contributor ⓘ

Lars Daniel covers digital evidence and cybersecurity in life and law.

Follow

0

Sep 25, 2024, 04:45pm EDT

Digital Forensics in the News

FORBES > INNOVATION > CYBERSECURITY

DoD Digital Forensics: Unlocking Evidence In Cars, Wearables, And IoT

Lars Daniel Contributor ⓘ

Lars Daniel covers digital evidence and cybersecurity in life and law.

FORBES > INNOVATION > CYBERSECURITY

Cracking Smartphone Passcodes In The Sean 'Diddy' Combs Case

Lars Daniel Contributor ⓘ

Lars Daniel covers digital evidence and cybersecurity in life and law.

Follow

0

Sep 24, 2024, 05:37pm EDT

Digital Forensics in the News

Digital evidence

Security cameras can deter criminals in the first place - and also help us identify them and bring them to justice.

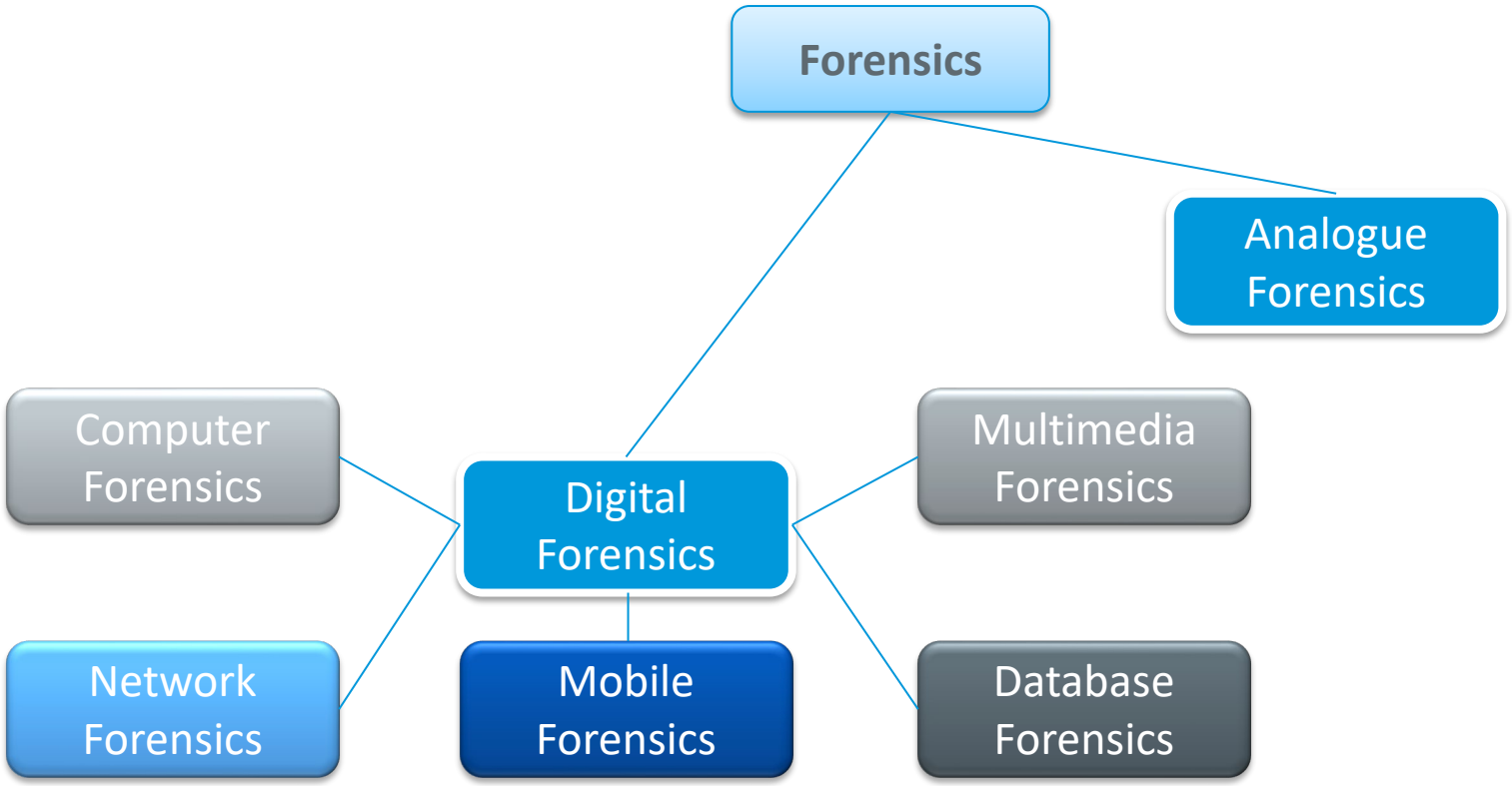
You can register your CCTV cameras or video doorbells on our secure digital evidence management system, NICE Investigate.

It's a quick and easy process. By registering, you will be set up to send us footage which we can use to catch criminals. **You'll be helping to keep your property and community safe.**

To register:

1. Send us an email to digitalevidence@northyorkshire.police.uk telling us that you would like to register your business or home security cameras.

Areas of Forensics



Adapted from R. Böhme , F. C. Freiling , T. Gloe , M. Kirchner, Multimedia Forensics Is Not Computer Forensics, Proceedings of the 3rd International Workshop on Computational Forensics, August 13-14, 2009, The Hague, The Netherlands

Why is Forensics & Security Difficult

- Managers unaware of value of computing resources
  - Thus, security of the resources may be underfunded
- Potential impacts sometimes too vague to quantify, e.g., damage to public image
- Legal definitions often vague or non-existent
- Legal prosecution is difficult
- Many subtle technical issues

Incident Management

- Security policy to manage security incidents
  - Detect security incidents
  - Appropriate response
- Need a plan
- Blue Team

Blue Team

- Defensive security
- Harden organisation's security
- Monitor for intrusions
- Perform Incident Response (IR)

- Prepare and improve IM plan
  - Update security policy after attack

Blue Team Knowledge

- Digital Forensics
- Vulnerabilities
- Threats
- Forensics and security toolkits

- Good communication skills

- Incident management and blue teams used combined contributions from **computer security** and **digital forensics** experts

HERIOT WATT UNIVERSITY

LEADERS IN IDEAS AND SOLUTIONS

Our lab study environment

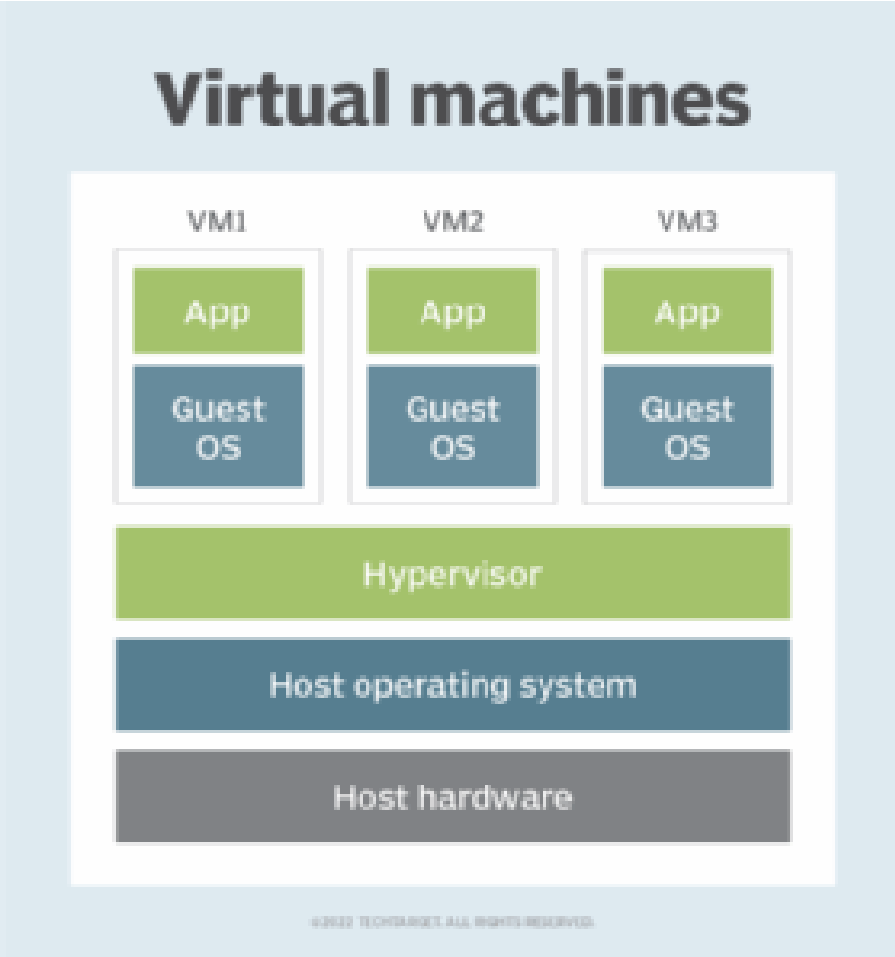
HERIOT WATT UNIVERSITY

Virtual Machines

- Digital Forensics investigations are typically performed in safe, controllable environments
- This often means using Virtual Machines (VMs)
  - Software that runs on a **host** computer that allows us to run a **guest** operating system
- For example, using the `virtualbox` VM software on a host machine*, you'll be able to run a Linux or Windows guest OS in the VM
  - Within the guest OS, you'll be able to execute commands and run some DF tools and applications

* In Dubai (lab 5.35) & Edinburgh (EM250 lab), `virtualbox` is preinstalled.

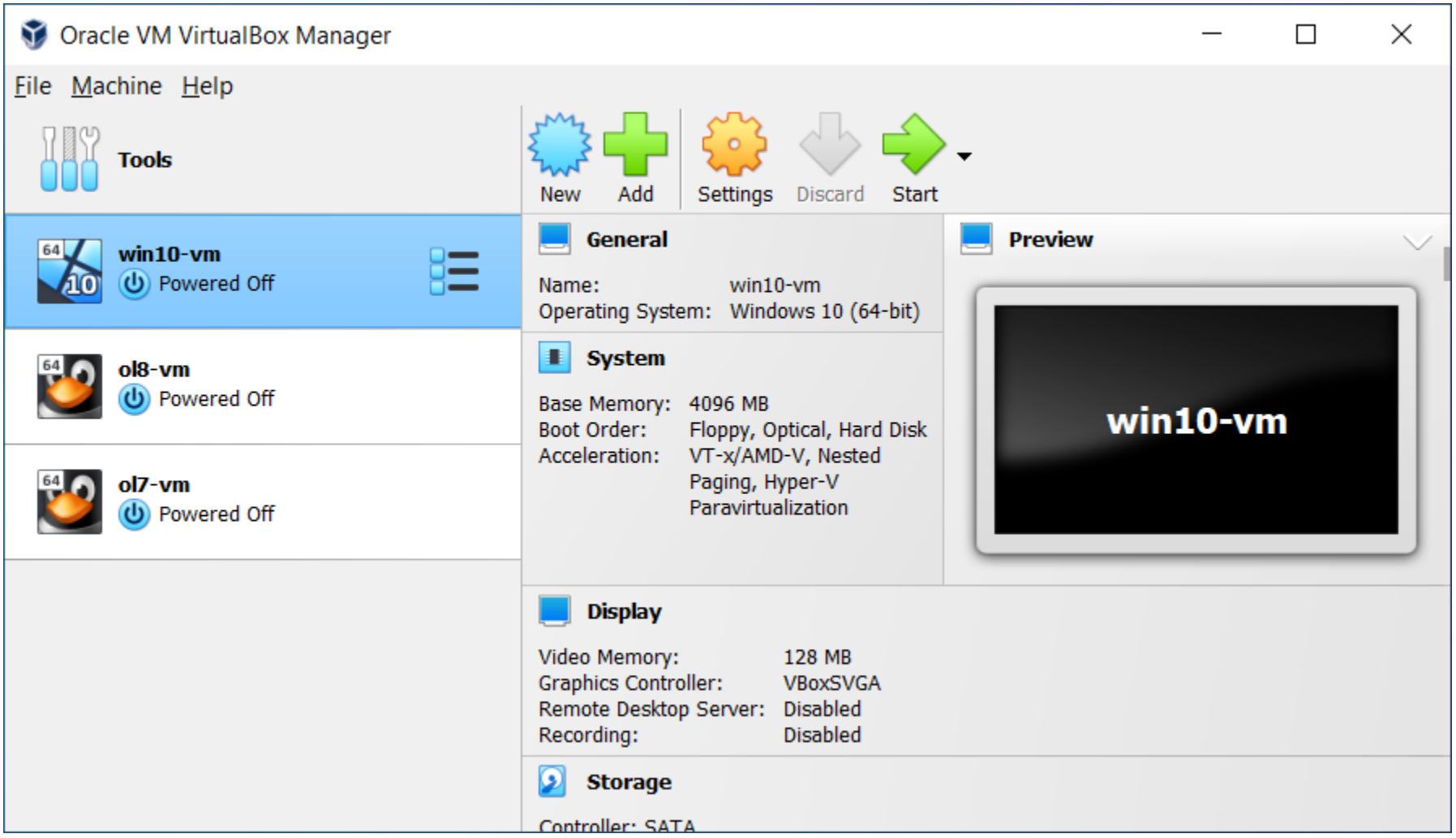
Virtual Machines



https://www.techtarget.com/searchitoperations/definition/virtual-machine-VM

HERIOT WATT UNIVERSITY

Virtual Machines



Disk Images

- A guest OS that is installed into the VM software is typically obtained as **disk image**
  - Often a `.iso` image, which is an optical disk image (e.g., software form on a DVD)
  - A sector-by-sector copy of a storage device
  - For example, you might download a `.iso` file of Kali Linux and load this into `virtualbox`, allowing you to run a Kali Linux VM on your host

Disk Images

- We also use disk images for digital forensics
- You might have a Windows VM running on your Linux host
- In the Windows VM you've installed some DF tools to analyse an Android disk image recovered from a crime scene
- Disk images for DF typically have different formats, and are bit-by-bit copies of a storage device
  - Raw (`.dd`) files. Physical disk copy created by Linux `dd`, and other applications.
  - Encase (`.E01`) files. A feature-rich physical copy of a storage device that supports inclusion of integrity data (e.g., hashes) and metadata (e.g., investigator notes) as part of the image file, and image compression. With a dd file, such information must be maintained or performed separately.

Disk Images

- Why are there special disk images for DF?
  - An `.iso` image is often file-system aware: it only copies sectors referenced by the file system, not including unallocated space. This is a *logical image*, not a *physical image.* Hence, `.dd` and `.E01` are preferred

Disk Images

- Virtual machines have their own disk formats
  - VMWare. Has a VMX (.vmx) “virtual machine configuration” file, that points to the main image content in a VMDK (.vmdk) “virtual machine disk” file
  - Virtualbox. Has VDI (.vdi) “virtual machine disk image” file. It can also import/export VMWare files.
- These aren’t disk images but rather support the portability of a VM.

Disk Images

- In your labs, you'll have an opportunity to use and create different disk images and VM files

Topic overview

- Topic 1 overview: Introduction to digital forensics
  - Computer security
  - Computer crimes
  - Digital evidence & forensics

Next topic

- Topic 2: Digital forensics & digital evidence
  - Digital forensics evolution
  - Digital investigations & evidence
  - Digital forensics tools