



Internet of Things (IoT) Forensics



Keith Cottenden CISSP

Head of Digital Forensics and Incident Response and a Certified Information Systems Security Professional with 3B Data Security. Responsible for overseeing PCI Forensic Investigations and Incident Response; addressing and managing the aftermath of a security breach or cyberattack.

Prior to this appointment, Technical Director at CYFOR for 15 years; responsible for directing all digital forensic operations within the company; providing specialist knowledge of information technology investigative techniques and dealing with complex evidential and legal issues, instructing investigating officers and counsel as appropriate; ensuring evidence continuity, evidential integrity and admissibility of any recovered evidence in a manner acceptable to a Court of Law.

Previously, Counter Intelligence Investigator in the Royal Air Force Police for 22 years.

Overview

The objective of traditional digital forensics is to identify, preserve, collect, analyse, interpret and present digital evidence, collected from various mediums, in a cyber related incident; the exponential growth of IoT devices and the increasing number of cyber security incidents has given birth to the term IoT forensics and the resulting challenges.

Digital Forensics

“Digital Forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”

Palmer G. A road map for digital forensic research. Technical Report DTR-T0010-01, DFRWS, November 2001. Report from the First Digital Forensic Research Workshop (DFRWS).

Internet of Things



The term Internet of Things generally refers to everything other than a computer or mobile device that could connect to the Internet.

But where does the line get drawn?





Kinkplay

Local seller | 11 sales

CELLMATE- Next Level App Controlled Remote Chastity Device- REGULAR

£104.99

Low in stock

VAT included (where applicable)

Add to basket



Almost gone. There's only 2 left and 18 other people have this in their basket right now.

Highlights

Handmade

Delivery and return policies

Ready to dispatch in

Cost to deliver

1 business day

Free



IoT Devices

- Smart TV's; smart speakers
- Home automation, CCTV, air conditioning, lighting, smart meters, locks
- Commercial security systems
- Wireless Sensor Networks (WSN)
- Use of mobile phones to interact with the real world (e.g. sensing)
- Devices that connect via Bluetooth enabled mobile phones to the Internet
- Connected Cars
- RFID enabled tracking
- Low power embedded systems
- Wearables



INTERNET OF THINGS

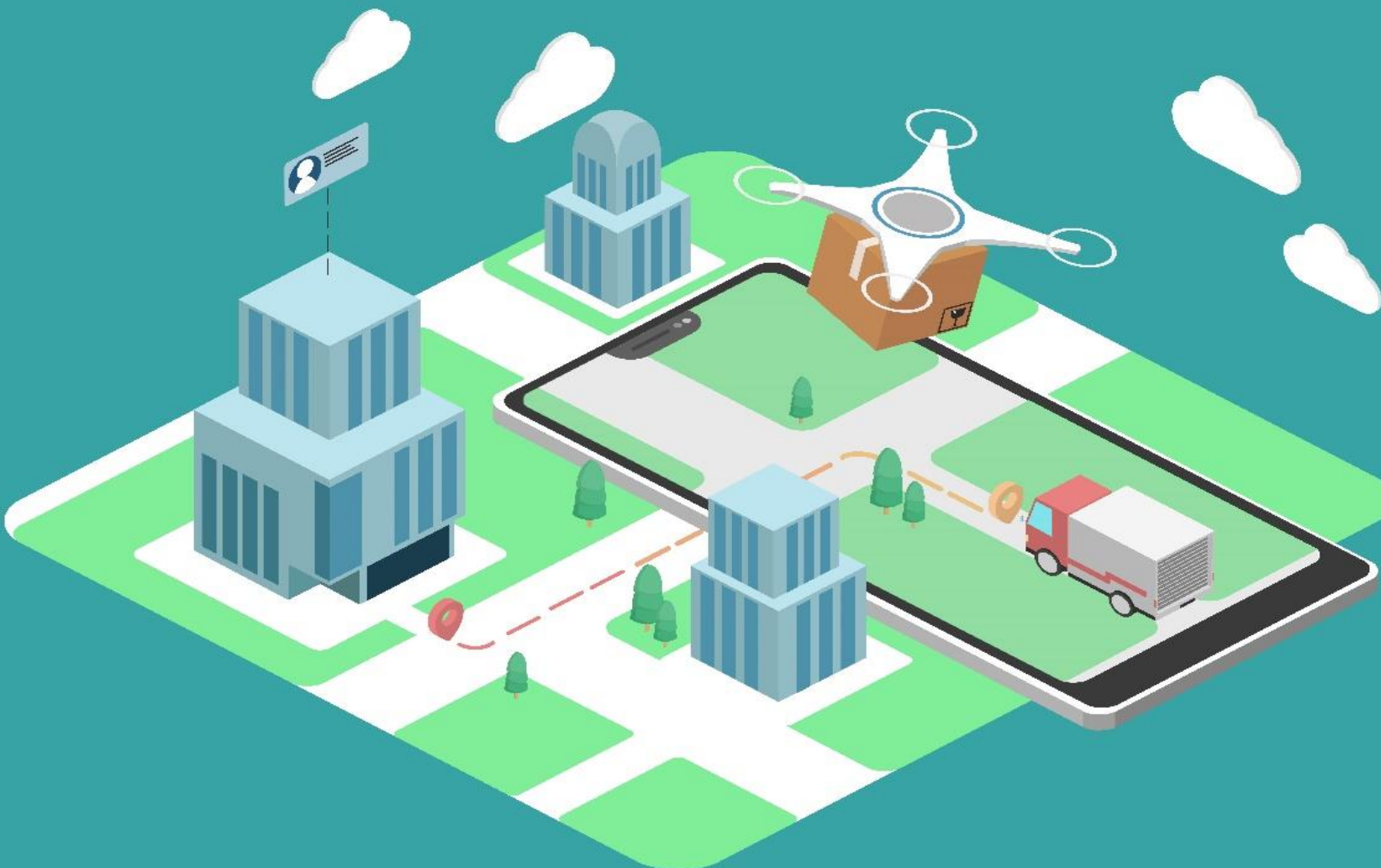




IoT devices generate and retain data artefacts that can be critical to a forensic investigation.



When compared to the standard digital forensic techniques, IoT forensics portrays multiple challenges depending on the versatility and complexity of the IoT devices.



Challenges

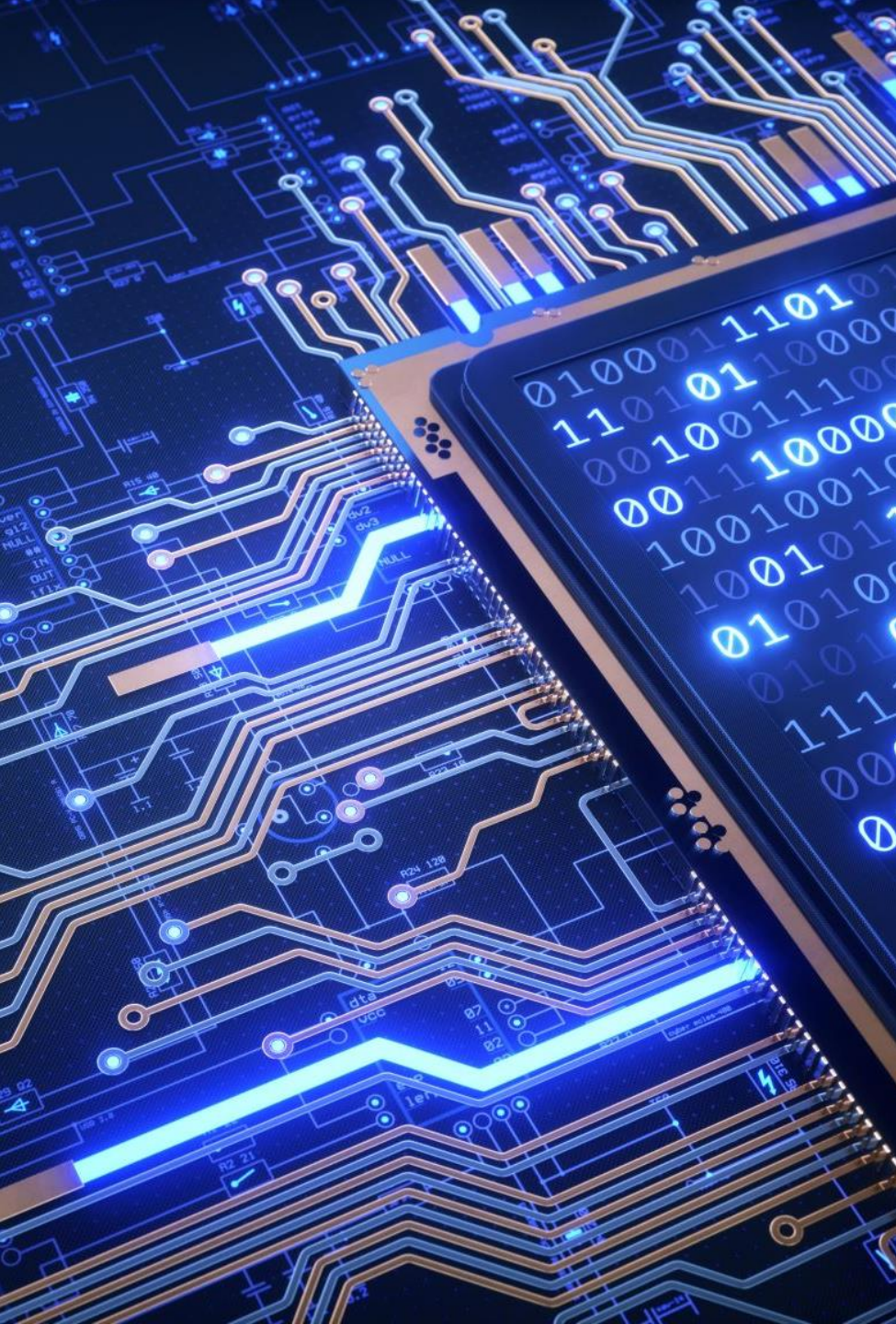
- **Variance of IoT devices;**
- **Proprietary hardware and software;**
- **Data present across multiple devices and platforms;**
- **Data can be updated, modified, or lost;**
- **Data location, stored on cloud or a different jurisdiction;**
- **Data format;**
- **Limitation of storage space; big data;**
- **IoT devices not supported by current digital forensic software.**

Approach

Develop a method in which data can be acquired and utilised in the analysis of forensic investigations while still considering laws and procedures that are currently in place.

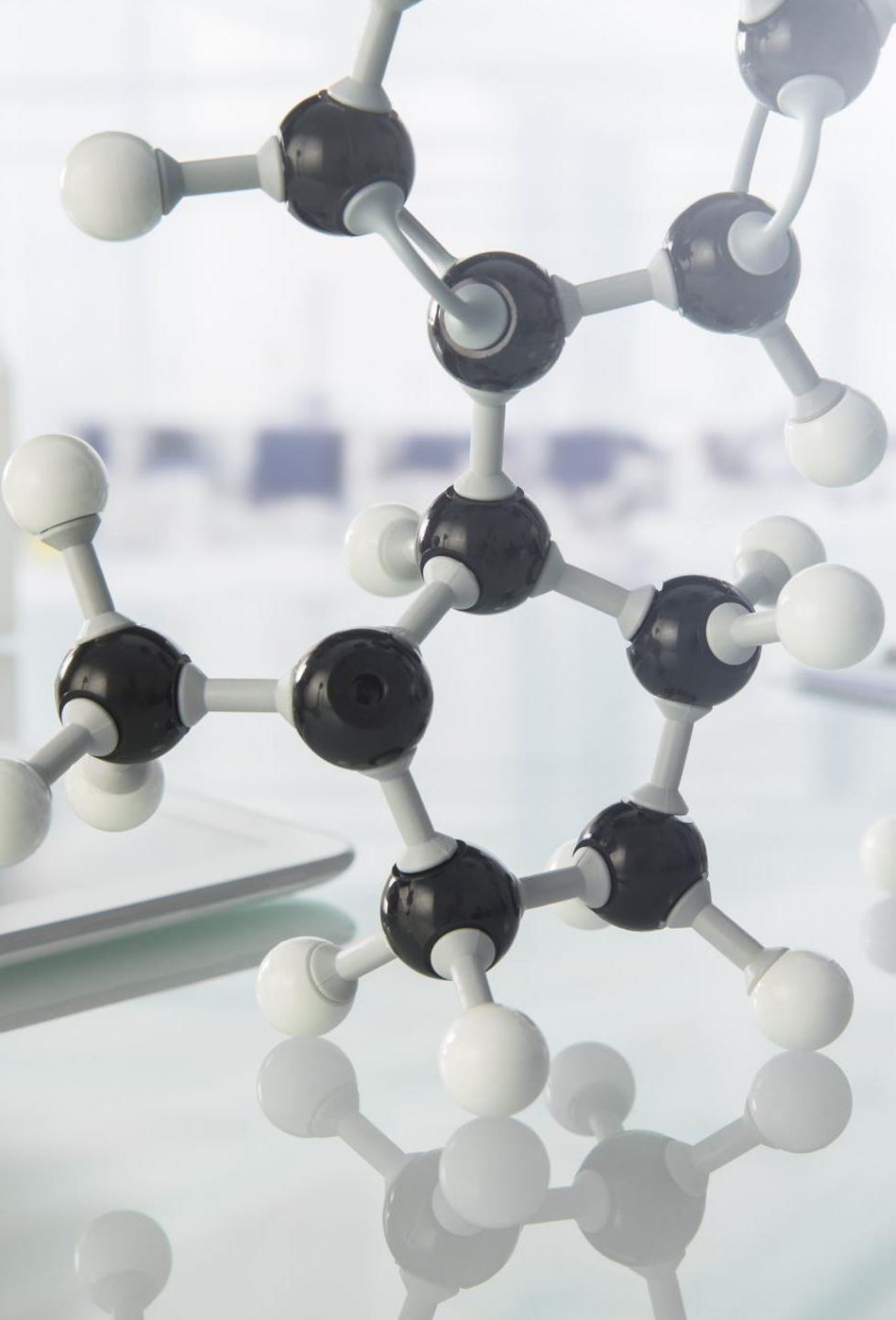
Potential sources of evidence include:

- **Smart devices and sensors;**
- **Hardware and Software;**
- **External resources.**



Conclusion

Most IoT devices come with no inbuilt security features and there is a requirement for more research into IoT devices security, IoT forensic readiness, and a forensic framework for IoT device.



Case Study - Medical Devices

- Bluetooth
- Windows
- Cloud
- Ethernet
- Wireless Keyboards

IoT Vulnerabilities

- **Default, weak, and hardcoded credentials**
- **Difficult to update firmware and OS**
- **Lack of vendor support and interest**
- **Vulnerable web interfaces (SQL injection, XSS)**
- **Coding errors (buffer overflow)**
- **Clear text protocols and open ports**
- **DoS / DDoS**
- **Theft and tampering**

Finally:

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account

Getting Started



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

<https://www.shodan.io/>

Cyber Incident Response
Digital Forensic Investigations
Digital Forensic & IR Retainers
IR Table Top & First Responder Training
Incident Response Policy Planning
ISO27001 & GDPR Consultancy
PCI DSS Consultancy & Compliance
Cardholder Data & PII Discovery
Penetration Testing
Virtual CISO



FORENSICS AND INCIDENT RESPONSE SERVICES

Forensics & Incident Response (Forensics)

Digital Forensic Investigations

IP Theft / Computer Misuse / Harassment

Data Recovery / Secure Destruction

Mobile Phone Investigations

Cardholder & PII Data Discovery

Litigation Support & eDiscovery Assistance

Cyber Liability / Insurance Markets

Forensics & Incident Response (IR)

Incident Response, Breach &
Data Compromise Investigations

PCI Forensic Investigator (PFI)

IR Workshops & Planning

IR First Responder & Breach Prevention Training

IR Policy Planning & Playbook Creation

IR Table-Top Exercises

IR Data Compromise Assessments





3B DATA SECURITY

KEITH COTTENDEN

3B DATA SECURITY

KEITH.COTTENDEN@3BDATASEcurity.COM

