Training Course on Smart City Infrastructure Forensics

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

This highly specialized training course is meticulously crafted for digital forensic investigators, cybersecurity professionals, critical infrastructure protection teams, and law enforcement agencies grappling with the unique investigative challenges presented by Smart City infrastructure. As urban environments rapidly integrate IoT devices, sensors, AI-powered systems, intelligent transportation networks, smart grids, and centralized control systems, they become increasingly susceptible to sophisticated cyberattacks and digital incidents. Training Course on Smart City Infrastructure Forensicsprovides the advanced knowledge and practical skills required to acquire, preserve, and analyze digital evidence from these highly interconnected and often proprietary systems, which are vital for uncovering the truth behind cyber-physical attacks, data breaches, and service disruptions in smart urban environments.

The curriculum delves into the complex interdependencies of Smart City components, ranging from IoT endpoints and cloud-based platforms to Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks that underpin critical services. Through hands-on labs, simulated attack scenarios, and real-world case studies, participants will learn how to navigate diverse data sources, analyze non-traditional forensic artifacts, and reconstruct events across vast, distributed networks. The course also critically examines the significant privacy implications of ubiquitous data collection and the legal frameworks (including Kenya's Data Protection Act 2019) governing data acquisition in smart cities, ensuring that all investigative practices are forensically sound, legally admissible, and ethically compliant, empowering organizations to safeguard the resilience and security of their urban ecosystems.

Programme Curriculum

Training Course on Smart City Infrastructure Forensics

Introduction

This highly specialized training course is meticulously crafted for digital forensic investigators, cybersecurity professionals, critical infrastructure protection teams, and law enforcement agencies grappling with the unique investigative challenges presented by Smart City infrastructure. As urban environments rapidly integrate IoT devices, sensors, AI-powered systems, intelligent transportation networks, smart grids, and centralized control systems, they become increasingly susceptible to sophisticated cyberattacks and digital incidents. Training Course on Smart City Infrastructure Forensicsprovides the advanced knowledge and practical skills required to acquire, preserve, and analyze digital evidence from these highly interconnected and often proprietary systems, which are vital for uncovering the truth behind cyber-physical attacks, data breaches, and service disruptions in smart urban environments.

The curriculum delves into the complex interdependencies of Smart City components, ranging from IoT endpoints and cloud-based platforms to Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks that underpin critical services. Through hands-on labs, simulated attack scenarios, and real-world case studies, participants will learn how to navigate diverse data sources, analyze non-traditional forensic artifacts, and reconstruct events across vast, distributed networks. The course also critically examines the significant privacy implications of ubiquitous data collection and the legal frameworks (including Kenya's Data Protection Act 2019) governing data acquisition in smart cities, ensuring that all investigative practices are forensically sound, legally admissible, and ethically compliant, empowering organizations to safeguard the resilience and security of their urban ecosystems.

Course Duration

5 Days

Course Objectives

1. Understand the architecture and interconnectedness of diverse Smart City infrastructure components (IoT, ICS/SCADA, cloud, communication networks).
2. Identify unique digital evidence sources within Smart City ecosystems, beyond traditional IT environments.
3. Perform forensically sound data acquisition from various Smart City devices, including IoT sensors, smart meters, and connected vehicle systems.
4. Analyze log data and network traffic from Smart City networks for indicators of compromise (IOCs) and attack vectors.

5. Investigate cyber-physical attacks impacting critical infrastructure (e.g., smart grids, water systems, traffic control).
6. Understand and apply ICS/SCADA forensic methodologies to industrial control systems within smart cities.
7. Extract and interpret geospatial data and video analytics from smart city surveillance and traffic management systems.
8. Identify vulnerabilities and attack surfaces specific to Smart City IoT devices and communication protocols.
9. Reconstruct complex incident timelines by correlating evidence from heterogeneous Smart City data sources.
10. Navigate data privacy challenges and comply with legal frameworks (e.g., Kenya Data Protection Act 2019) when investigating Smart City data.
11. Utilize specialized forensic tools and platforms for large-scale, diverse data analysis in Smart City environments.
12. Develop proactive forensic readiness strategies for Smart City infrastructure to enable rapid incident response.
13. Generate comprehensive forensic reports detailing findings from complex Smart City investigations, suitable for legal proceedings.

Organizational Benefits

1. Enhanced Critical Infrastructure Protection: Proactively identify and respond to cyber threats targeting essential urban services.
2. Improved Incident Response Capabilities: Rapidly investigate and mitigate the impact of cyber-physical attacks on Smart City systems.
3. Proactive Threat Intelligence: Develop internal expertise to identify vulnerabilities and emerging threats unique to Smart City infrastructure.
4. Reduced Financial & Reputational Risk: Minimize the impact of data breaches, service disruptions, and public safety incidents.
5. Strengthened Compliance: Ensure data collection and analysis practices align with privacy laws (e.g., Kenya Data Protection Act) and industry standards.
6. Optimized Security Operations: Equip security teams with specialized skills for a complex and rapidly evolving threat landscape.
7. Data-Driven Decision Making: Leverage forensic insights to inform policy, investment, and security improvements for Smart Cities.
8. Cross-Sector Collaboration: Facilitate better understanding and cooperation between IT, OT, and physical security teams.
9. Increased Public Safety: Contribute to the overall security and resilience of urban environments for citizens.

10. Leadership in Smart City Security: Position the organization as a leader in securing and investigating advanced urban technologies.

Target Participants

- Digital Forensic Investigators
- Cybersecurity Incident Responders
- Critical Infrastructure Security Specialists
- Law Enforcement (Cybercrime, Emergency Services)
- SCADA/ICS Security Professionals
- Smart City Planners and Architects (with a security focus)
- IoT Security Researchers
- Government Regulatory Bodies
- Urban Data Analysts (with a forensic interest)
- Threat Intelligence Analysts

Course Outline

Module 1: Introduction to Smart City Architecture & Forensics (Smart City Forensics Fundamentals)

- Defining Smart Cities: Components, Goals, and Challenges
- Smart City Reference Architectures (e.g., IoT Layers, Communication Networks)
- Unique Forensic Challenges in Smart City Environments (Scale, Diversity, Real-time Data)
- Legal and Ethical Considerations in Smart City Data Collection (Kenya Data Protection Act)
- **Case Study**: Mapping the interconnected systems of a typical "smart street light" deployment.

Module 2: IoT Device Forensics in Smart Cities (Smart City IoT Forensics)

- Types of IoT Devices in Smart Cities (Sensors, Cameras, Smart Meters, Wearables)
- Data Acquisition Techniques for Diverse IoT Endpoints (On-device, Gateway, Cloud)
- Analyzing IoT Device Logs, Firmware, and Communication Protocols
- Identifying Compromised IoT Devices and Botnet Indicators
- **Case Study**: Extracting and analyzing data from a smart public safety camera after a security incident.

Module 3: ICS/SCADA Forensics in Critical Urban Infrastructure (SCADA Forensics)

- Overview of Industrial Control Systems (ICS) and SCADA in Smart Cities (Utilities, Traffic)

- Unique Characteristics of SCADA Networks and Protocols (Modbus, DNP3, IEC 61850)
- Data Acquisition from PLCs, RTUs, and HMI Systems
- Forensic Analysis of SCADA Logs, Alarms, and Control Commands
- **Case Study**: Investigating a cyber-attack on a smart water management system using SCADA logs.

Module 4: Smart City Network & Cloud Forensics (Smart City Network Forensics)

- Analyzing Communication Networks: 5G, Wi-Fi, LPWAN (LoRaWAN, NB-IoT)
- Intercepting and Analyzing Network Traffic within Smart City Ecosystems
- Cloud-Based Data Storage and Processing in Smart Cities (AWS, Azure, Google Cloud)
- Forensic Challenges of Multi-Tenant Cloud Environments
- **Case Study**: Tracing anomalous data exfiltration from a smart traffic sensor network to a cloud server.

Module 5: Data Analytics & Visualization for Smart City Forensics (Smart City Data Analysis)

- Managing and Analyzing Large Volumes of Heterogeneous Smart City Data
- Geospatial Analysis of Location Data from Sensors and Vehicles
- Video Forensics from Smart City Surveillance Systems
- Correlating Data from Disparate Sources for Timeline Reconstruction
- **Case Study**: Using GIS tools to visualize the movement of a suspicious vehicle captured by multiple smart cameras.

Module 6: Cyber-Physical Attack Investigations (Cyber-Physical Attack Forensics)

- Understanding Attack Vectors in Smart City Environments (Supply Chain, Ransomware, DDoS)
- Investigating Attacks Targeting Physical Infrastructure (e.g., power grid manipulation, traffic signal disruption)
- Detecting and Responding to Compromises in Integrated IT/OT Systems
- Damage Assessment and Remediation Strategies for Cyber-Physical Incidents
- **Case Study**: Analyzing evidence from a ransomware attack that impacted public transportation systems.

Module 7: Proactive Forensic Readiness for Smart Cities (Smart City Forensic Readiness)

- Developing Forensic Readiness Plans for Smart City Infrastructure
- Implementing Logging and Monitoring Strategies for IoT and ICS Devices
- Establishing Data Governance and Retention Policies for Smart City Data
- Building Incident Response Playbooks Specific to Smart City Threats
- **Case Study**: Designing a logging strategy for a new smart energy grid deployment to ensure forensic visibility.

Module 8: Legal, Policy & Future Trends in Smart City Forensics (Smart City Legal & Future)

- Legal Obligations and Regulatory Compliance in Smart City Data Handling (Kenya Data Protection Act 2019)
- Cross-Border Data Challenges and International Cooperation
- Ethical Implications of Surveillance and Data Collection in Smart Cities
- Emerging Technologies: AI in Smart Cities, Digital Twins, Quantum Computing and their Forensic Impact
- **Case Study**: Discussing the legal and ethical considerations of using smart city surveillance footage for criminal investigations in Kenya.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com