IPv6 Forensics

How to prepare for and carry out forensics investigations involving IPv6 networks and devices. **(4 days)**

Relevant Platforms:

- **Cisco IOS**
- **Juniper JunOS**
- **HP**
- **Linux**
- **Unix**
- **FreeBSD**
- **Microsoft Windows**

You will learn:

- How to undertake a forensic investigation
- The principles of digital and network forensics
- Details of the core IPv6 protocols
- How IPv6 networks operate
- How to interpret IPv6 addresses
- The basics of IPv6 security
- How IPv6 forensics differ from IPv4 and general network forensics
- How to obtain and analyse IPv6 address
- How to capture IPv6 traffic
- How to analyse IPv6 traffic & related protocols
- When and how to use traffic capture tools such as Wireshark and tcpdump
- Other sources of traffic information such as flow analysis and NetflowV9
- How to analyse IPv6 traffic flows
- Where to obtain IPv6 network forensics data in different network nodes
- How to capture and analyse IPv6 application protocols and data
- Capturing forensics information for network devices such as switches, routers and firewalls
- How to carry out advanced IPv6 forensics investigations dealing with specific IPv6 attacks
- How to carry out advanced IPv6 forensics investigations dealing with IPv6 transition scenarios

Course Benefits

IPv6 is steadily replacing IPv4 as the network protocol that underpins the global Internet. The deployment of IPv6 brings with it the need to be able to carry out forensics investigations on IPv6 networks, network devices, nodes and applications.

In this course, you will learn the fundamentals of digital forensics, network forensics and the details of how you should apply these to IPv6 networks.

You will learn the types of evidence available to you in IPv6 networks, where you can obtain it, how you should acquire it and how you can interpret it.

You will also gain experience with using a wide variety of tools to collect and analyse IPv6 evidence on networks and devices.

Who Should Attend

This course is aimed and security, forensic and law enforcement professionals responsible for forensics in modern IPv6 enabled networks.

The techniques and tools taught in this cause will also be of interest to a wider audience of networking professionals whose roles include network security and incident response.

A good knowledge of general networking concepts is assumed. Previous training and experience in IPv6 is recommended.

Whilst this course focuses on IPv6, many of the techniques and tools are also equally applicable to legacy IPv4 networks.

Course Contents

IPv6 Forensics Fundamentals

- The purpose and definition of forensics
- Principles of forensics
- Legal and ethical considerations
- Evidence and best evidence
- Footprints
- Challenges of modern forensics
- Digital forensics overview
- Network forensics overview
- Course overview and introduction

Sources of IPv6 Evidence

- Overview of sources of IPv6 evidence
- IPv6 addresses and IPv6 multicast
- The IPv6 protocol
- The neighbor discovery protocol (ND)
- ICMPv6
- IPv6 address autoconfiguration
- SLAAC and DHCPv6
- IPv6 transition mechanisms
- IPv6 features (IPsec, mobility and QoS)
- IPv6 security features
- Name resolution and DNS
- IPv6 applications
- IPv6 nodes; switches, routers and other devices

Interpreting IPv6 Addresses

- Why IPv6 addresses are important in forensics
- The structure of IPv6 addresses
- How IPv6 and IPv4 addresses differ
- Overview of IPv6 address types
- Sources of IPv6 address evidence
- Reserved IPv6 addresses and prefixes
- IPv6 address interface identifiers (IIDs)
- Modified EUI-64
- Privacy, opaque and temporary Addresses
- CGAs and HBAs
- Transition addresses
- Understanding IPv6 prefixes
- Interpreting IPv6 addresses
- Tracing the source of an IPv6 address
- Implications for IPv6 address management

IPv6 Traffic Capture & Analysis

- The role of traffic capture
- IPv6 protocol capture and analysis
- Overview of packet capture tools
- How to use Wireshark with IPv6
- How to use tcpdump with IPv6
- IPv6 capture filters
- Other traffic capture tools
- Analysis of IPv6 packets
- Advanced IPv6 traffic capture techniques
- Intrusion detection and analysis
- Flow analysis
- Upper layer analysis
- Preparation for traffic capture
- Large scale traffic capture

IPv6 Flow Capture & Analysis

- Acquiring flow data
- Overview of flow information sources
- IPv6 flow analysis
- NetFlow collection and analysis
- NetFlow v9 and IPv6
- Flow capture components
- Overview of open-source flow tools
- Using open-source tools to examine flows
- nfcapd, nfpcapd, and nfdump
- SOF-ELK: NetFlow ingestion and dashboards
- Examples of IPv6 flows analysis

Evidence from Neighbor Discovery (ND)

- ND overview
- Sources of ND evidence
- Stateless Address Autoconfiguration (SLAAC)
- Relationship to DHCPv6
- The RDNSS & DNSSL options
- Detecting specific ND attacks
- ND security tools
- ND inspection & MLD snooping
- Secure Neighbor Discovery (SeND)
- Acquiring ND evidence
- Interpreting ND evidence
- ND on hosts, switches and routers

DHCPv6 Forensics

- Overview of DHCPv6
- DHCPv6 as a source of address evidence
- Obtaining DHCPv6 state information
- DHCPv6 logs
- Capture and analysis of DHCPv6 traffic
- DHCPv6-shield in switches
- Other DHCPv6 security tools
- Detecting DHCPv6 attacks and misuse
- Examining a node's DHCPv6 state
- DHCPv6 and DDI (DHCPv6, DNS and IPAM)

IPv6 Name Resolution and Forensics

- Overview of IPv6 name resolution
- Complexities from use of two protocols
- Relationship with transition mechanisms
- Interpreting DNS logs
- Capture and analysis of DNS traffic
- Detecting specific attacks against DNS
- Fast flux
- Domain name generation algorithms (DGAs)
- DNS tunnelling
- Examining a node's name resolution state
- DNS and name resolution tools

IPv6 Transition Forensics

- Overview of IPv6 transition mechanisms
- 6over4, 6to4, 6rd, ISATAP, Teredo, DSLite
- NAT46, NAT64, DNS64, 464XLAT
- IPv6 dual stack operation
- Common IPv6 transition scenarios
- Forensic and transition mechanisms
- Obtaining evidence from transition mechanisms
- Capture and analysis of transition traffic
- Transition mechanism security
- Detecting attacks via transition mechanisms
- Legacy mechanisms

IPv6 Application Forensics

- IPv6 implications for application forensics
- Overview of sources of application evidence
- Capturing and interpreting application traffic
- Logging and log aggregation
- Syslog and eventing
- Microsoft protocols
- IPv6 SMTP and interpreting SMTP logs
- IPv6 HTTP and Interpreting HTTP logs
- Application proxies
- Content Delivery Networks (CDNs)
- Largescale log analytics

IPv6 IPsec Forensics

- Overview of IPsec
- Implications for forensics
- Implications for firewalls
- IPsec traffic capture and analysis
- IPsec flow analysis

IPv6 Network Evidence

- Dynamic routing information
- RIPng, OSPFv3, IS-IS, EIGRPv6, BGP4, PIM
- Firewall log monitoring
- Intrusion detection system (IDS) logs
- Network security monitoring logs
- Syntax and log formats
- Rules and signatures
- Families of IDS and NSM solutions

Company Registration: 3521142

VAT Number: 698 3633 78

Hands-on IPv6 Practical Labs

Each module includes detailed exercises. The course is generic and covers material relevant to many platforms. Delegates undertake most lab work on Linux.

Hands-on IPv6 forensics practical exercises include:

- Examining and understanding IPv6 networks
- Analysing and interpreting IPv6 addresses
- Capturing and analysing IPv6 packets
- Tracing IPv6 traffic back to the source
- Using Wireshark to capture IPv6 packets
- Using tcpdump to capture IPv6 packets
- Using tools to filter and interpret IPv6 traffic
- Acquiring IPv6 flow data using a range of tools
- Collecting NetFlowv9 flow data
- Analysing and interpreting NetFlow data
- Using open-source NetFlow tools
- Large scale analysis of IPv6 flows
- Using SOF-ELK
- Detecting and analysing Neighbor Discovery attack traffic
- Using and understanding ND security tools
- Acquiring ND evidence from nodes, switches and routers
- Obtaining and using DHCPv6 state information
- Capturing and analysing DHCPv6 traffic
- Understanding the role of name resolution in IPv6 forensics
- Examining DNS logs
- Detecting DNS attacks
- Acquiring evidence from IPv6 transition mechanisms
- Capturing and interpreting transition mechanism traffic
- Carrying out IPv6 application forensic evidence collection and analysis
- Interpreting Email Logs
- Interpreting web server, web proxy and content delivery network logs
- Capturing and dissecting IPv6 IPsec traffic
- Collecting relevant evidence from security devices such as firewalls and IDS
- Filtering and interpreting firewall logs
- Practice detecting common IPv6 attacks

The IPv6 Trainers

Trainers are practising IPv6 consultants with extensive experience of IPv6. Further information can be found at www.erion.co.uk.

Erion is the world's leading IPv6 training company.

Erion
Certified IPv6 Training