endace
accelerated

Electronic evidence:
Worth it's weight in gold?

endace – power to see all

endace
accelerated

europe
P +44 1223 370 176
E eu@endace.com

americas
P +1 703 964 3740
E usa@endace.com

asia pacific
P +64 9 262 7260
E asia@endace.com

technology
P +64 7 839 0540
E nz@endace.com

Presenter

Greg Howard

Vice-President EMEA

Endace Europe Ltd

- Bio NZ/UK Dual National – Vice President Sales
- 17 years experience in hi-tech industry, primarily semiconductors and LCD Distribution in 3 geographies (EMEA, NZ and Australia)
- Joined Endace in April 2005
- Prior to Endace Managing Director Braemac Limited (1998-2005) Started up UK operation and developed it into a self sufficient $12m USD Business.

For captured communications to be credible evidence in a prosecution, it must be shown that a robust and reliable method was used to intercept that information. It is vital that a common yet undetectable technology is implemented to guarantee 100% capture of target flows on IP networks. After all, information is only as reliable as its source.

Agenda

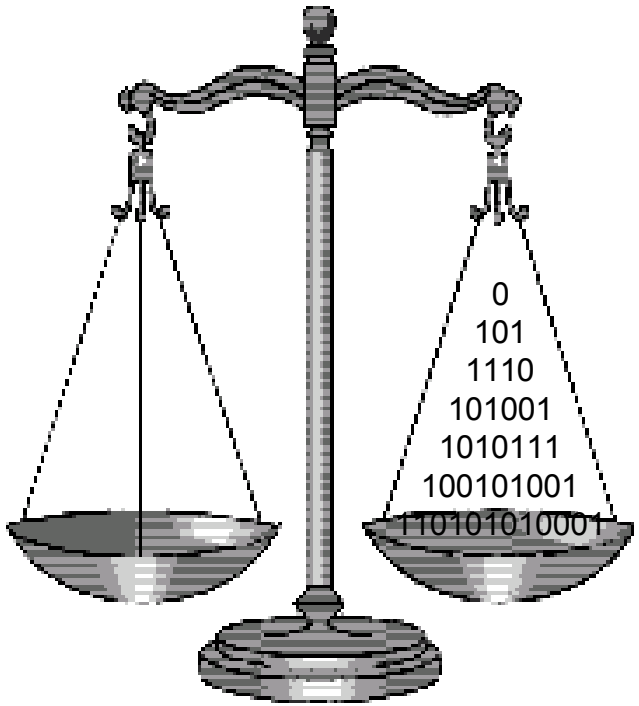
endace
accelerated

- How much do a few bytes of information weigh?
- Can you rely on electronic evidence?
- Requirements of intercept infrastructure
- Endace infrastructure for LI on IP networks
- How do you collect the data?
- How heavily do those bytes weigh in your investigation?
- Q&A

How much do a few bytes weigh?

endace accelerated

- Electronic communications on IP networks:
  - Weightless: Exists only ‘in the ether’ of the Internet, between 2 endpoints (people at computer terminals, laptops, PDAs, VoIP phones)
  - Difficult to target: No physical circuit to be intercepted, not even any virtual circuit to be intercepted. No simple ‘wiretap’ like a phone.
  - Fragmented: The communications are carried using a ‘connectionless’ network – they can be split over many different routing paths.



Can you rely on electronic evidence?

endace accelerated

- Depends on local legislation:
  - In some cases, yes, recordings of electronic communications can be lodged as evidence for prosecutions.
  - In other jurisdictions it is not admissible as evidence.
  - However, it can provide law enforcement with useful intelligence ('probable cause') to enable an investigation.

- The need is high, and the need is now:
  - Unfortunately, we now face threats to public security in many countries
  - Criminals are becoming increasingly intelligent at communicating covertly
  - The cost of failure is high (in lives, in reconstruction)
  - Well equipped and well informed Law Enforcement Agencies are crucial

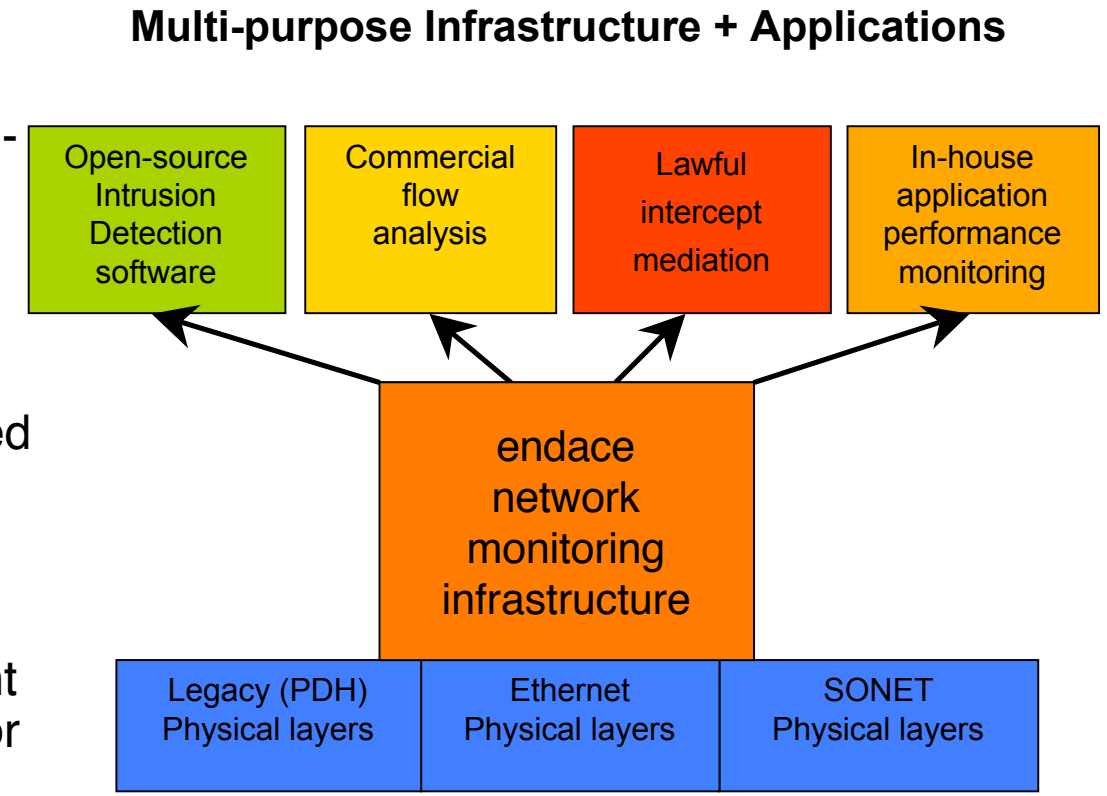
Requirements of intercept infrastructure

endace
accelerated

- Invisible: No-one on the network should be able to detect an interception, nor detect that the systems exist (ie. Must be hack-proof)
- Secure: Only authorised persons shall have access to the mediation layer, which securely controls the intercept infrastructure.
- Lossless: Must guarantee accurate recording of every byte of data to/from the targets.
- Manageable: Must be able to be deployed and controlled throughout large carrier networks, nationwide.
- Responsive: Intercepts must be implemented promptly after receiving a lawful request.
- Reasonable cost: Must provide a sound return on investment.

Endace infrastructure for LI on IP networks

- Internal network operations to intercept and record traffic are separated from the mediation layer(s). (ie. See ETSI model)
- The infrastructure is application-agnostic (any traffic analysis applications and LI mediation systems can be layered on top)
- Each analysis/intercept application is securely separated from the others.
- The infrastructure asset can be leveraged for the service provider's network management purposes, generating an ROI for them:
  - Manage service delivery
  - Offer revenue-generating security monitoring services



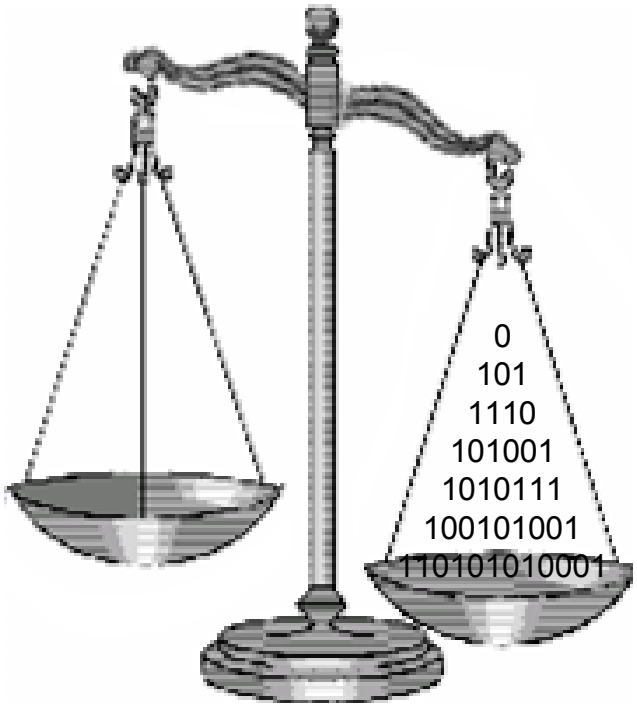
How do you collect the data?

- Endace network monitoring probes are connected to the network by passive taps.
  - They are invisible to the network, and have no MAC or IP address.
- Lossless high-precision recording to disk is guaranteed by Endace's DAG technology.
  - All packet time-stamps are accurate to <100 nanoseconds.
- Deployed at the 'edge' between the core network and access networks, individual lines can be targeted, and all traffic in/out is silently mirrored and recorded to disk.
  - This includes all network signalling information, all 'session' setups/tear-downs and the full content of all communications.
- Supported network types: Ethernet, ATM, PoS, PDH/TDM
  - The monitoring infrastructure can tap at any point in the carrier network.

How heavily do those bytes weigh?

endace
accelerated

- All communications are completely captured and accurately recorded, so there can be no doubt of the activities/communications of the target.
- We have the data stored in a reusable format, so it can be analysed and reassembled using many different tools.
- It is now only a question of the legal environment in which we operate.



Q&A

endace
accelerated

- What about protocol and session reassembly?
  - The recorded traffic is delivered natively by Endace monitoring probes as either standard PCAP files, or Endace Record Format (ERF).
    This provides a ‘raw’ record of all activity of the target without any modification.
  - A wide range of applications, commercial & open source, are able to use these files and reassemble the session content, enabling visibility into the content of the user’s activities. (Email, IM chat, webpages, etc.)
  - The LI mediation layer chosen is able to reassemble the raw traffic into the format necessary for easier analysis by the LEA. (eg. Summary of VoIP sessions made)