

# Network Forensics

## Gerald Combs

Creator, Wireshark (formerly Ethereal)

[www.wireshark.org](http://www.wireshark.org) | [www.cacotech.com](http://www.cacotech.com)

## Laura Chappell

Founder, Wireshark University/Chappell Seminars

[www.wiresharkU.com](http://www.wiresharkU.com) | [www.chappellseminars.com](http://www.chappellseminars.com)

**Want copies of slides?**

**[laura@chappellseminars.com](mailto:laura@chappellseminars.com)**

Wireshark  
is divine!



# The OHDDL Case

Subject: Kalon Tripa Succession  
From: "Pema Rinzin" <[prinzintibet@yahoo.com](mailto:prinzintibet@yahoo.com)>  
Date: Thu, September 18, 2008 8:14 am  
To: [choejor@dalailama.com](mailto:choejor@dalailama.com)

---

Dear Sir,

Attached please find the final Tibetan translation of my English announcement for the Kalon Tripa succession initiative. Response to my press release on September 2nd has been very positive and I have been receiving lots of email and phone messages from Tibetans everywhere.

I am trying to get someone to translate the Kalon Tripa Hochoe into English, but if you already have it translated, please send it to me.

Any advice from you in this initiative of mine would be greatly appreciated.


Yours sincerely,

Pema Rinzin  
President  
TAC

Official Photographer/webmaster  
Office of His Holiness the Dalai Lama  
Thekchen Choeling  
P/O Mcleod ganj 176219  
Dharamsala (H.P.)  
India

**Planting the  
Seed of Social  
Malware**

# Another Case of Interest

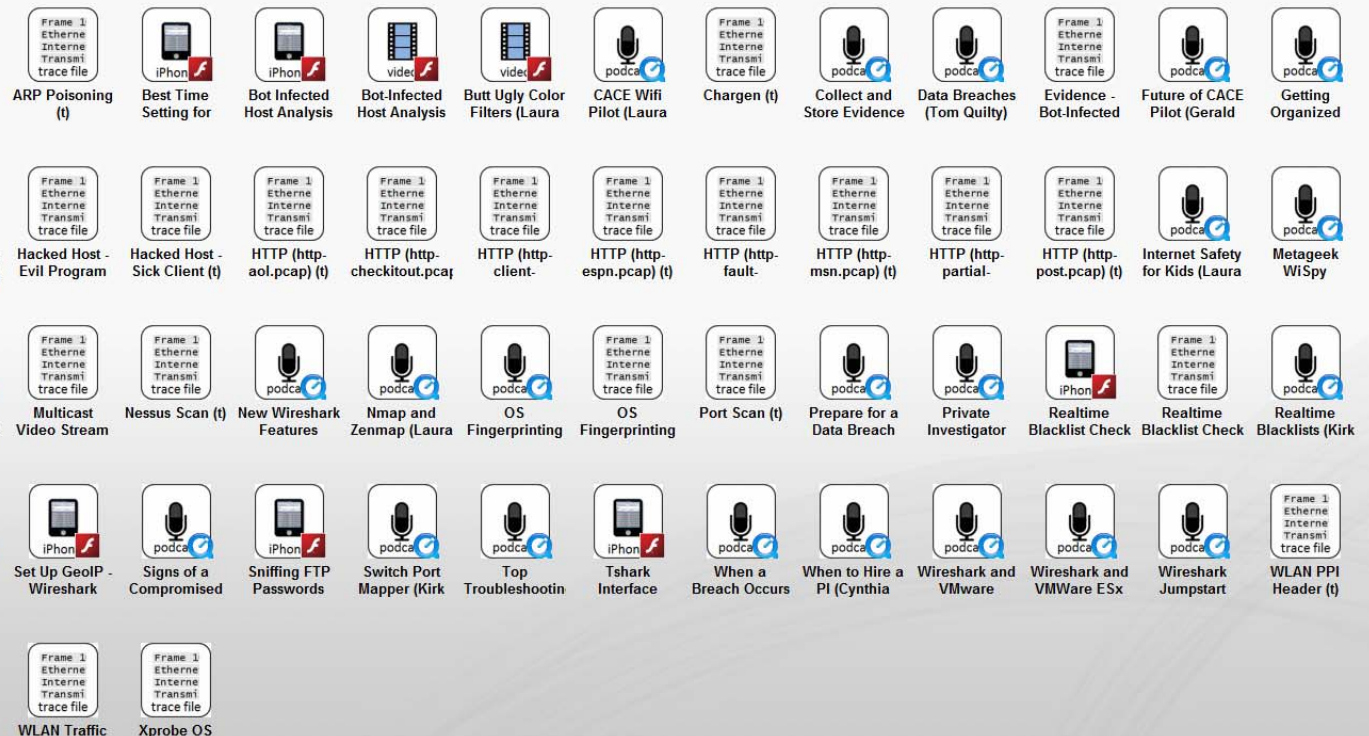
A photograph of a hotel reception desk. A woman in a black and white patterned top is behind the counter, talking to a blonde woman in a white shirt who is holding a black suitcase. The scene is set in a modern hotel lobby with wood-paneled walls.

**Here's your sense of false security... Enjoy your stay.**

**Thank goodness they have WEP on this WLAN!**

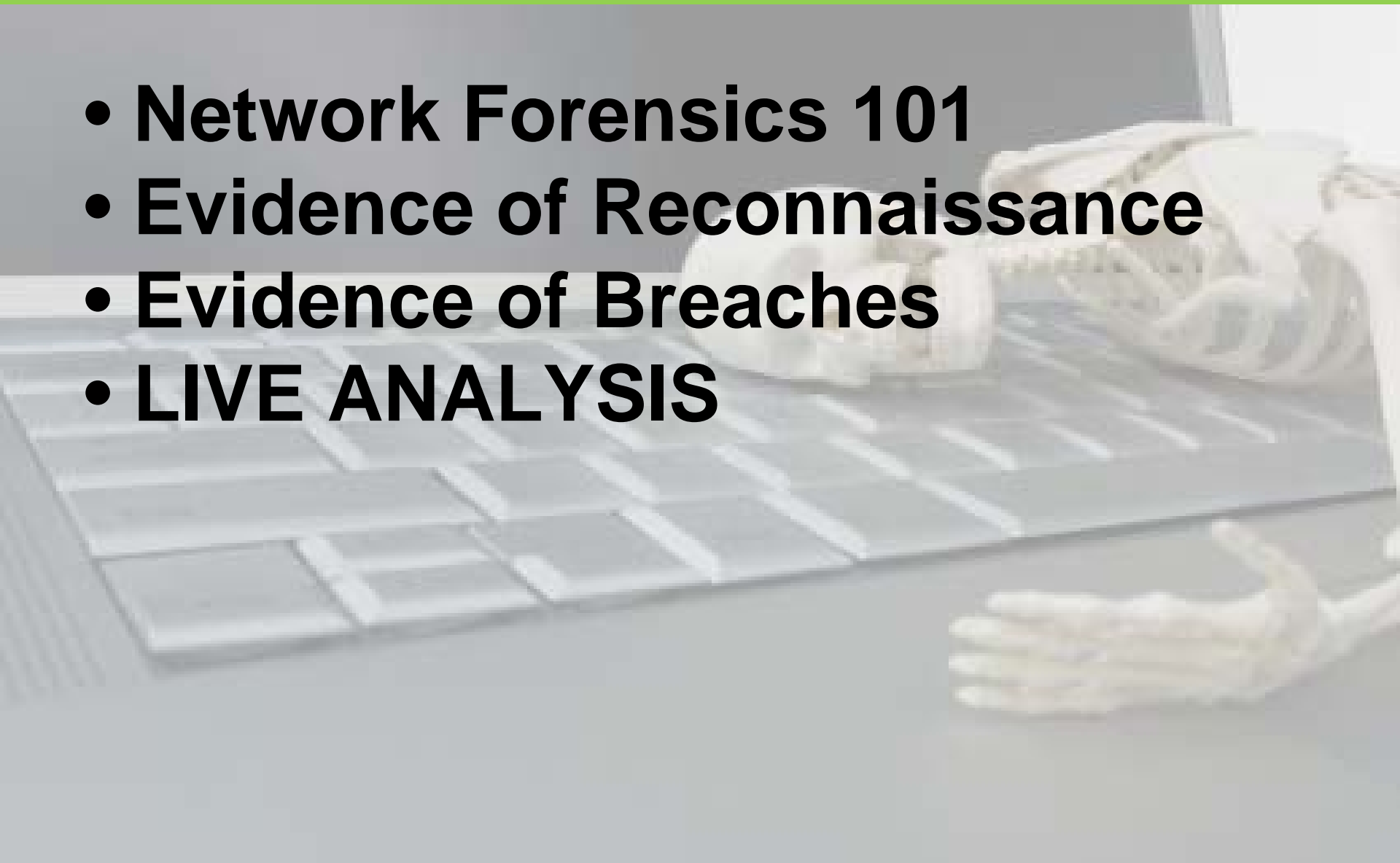
# Want Trace Files and More?

Laura's Media Roll at [chappellseminars.com](http://chappellseminars.com)  
[www.screencast.com/users/laurachappell](http://www.screencast.com/users/laurachappell)

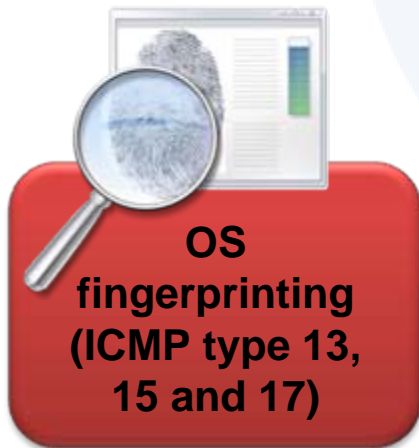
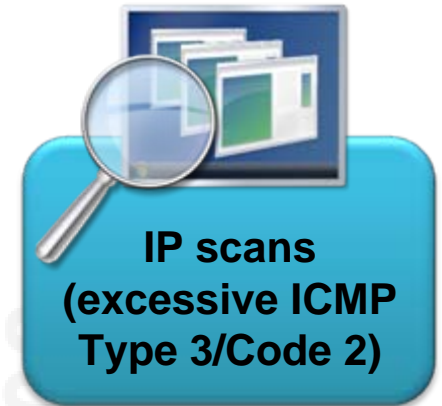
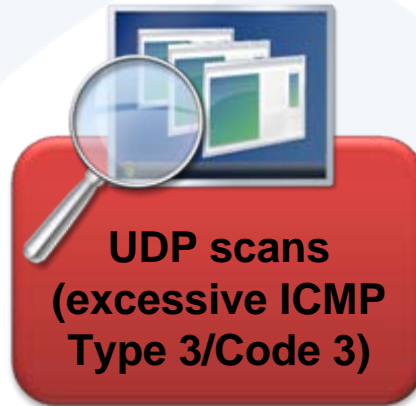
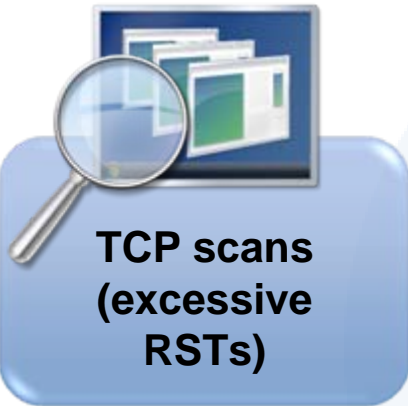


# In this Session

- **Network Forensics 101**
- **Evidence of Reconnaissance**
- **Evidence of Breaches**
- **LIVE ANALYSIS**



# Evidence of Reconnaissance



# Evidence of Breaches

! Unusual communication pairs

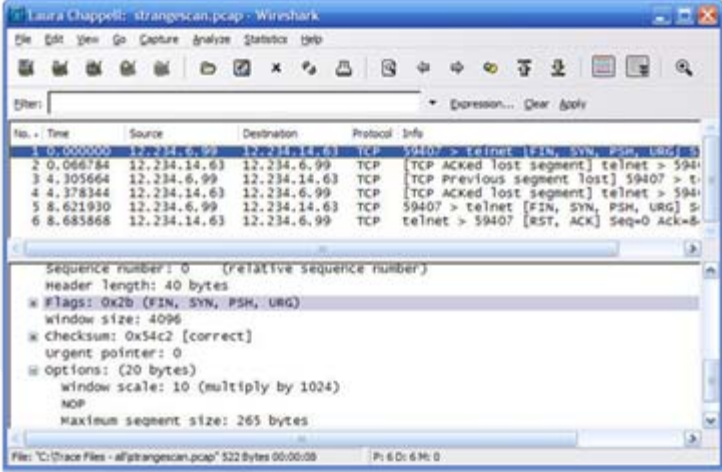
! Unusual protocols and ports

! Excessive failed connections

! Unusual inbound connections

! Unusual outbound connections

! Peer-to-peer traffic paths



The image shows a Wireshark window titled "Laura Chappell: strangescan.pcap - Wireshark". The main pane displays a list of network packets. The first six packets are TCP connections from source IP 12.234.14.63 to destination IP 12.234.6.99. The protocols are all TCP, and the info column shows telnet connections. Packet 6 is a RST, ACK packet with Seq=0 and Ack=6. The packet details pane shows the following information:

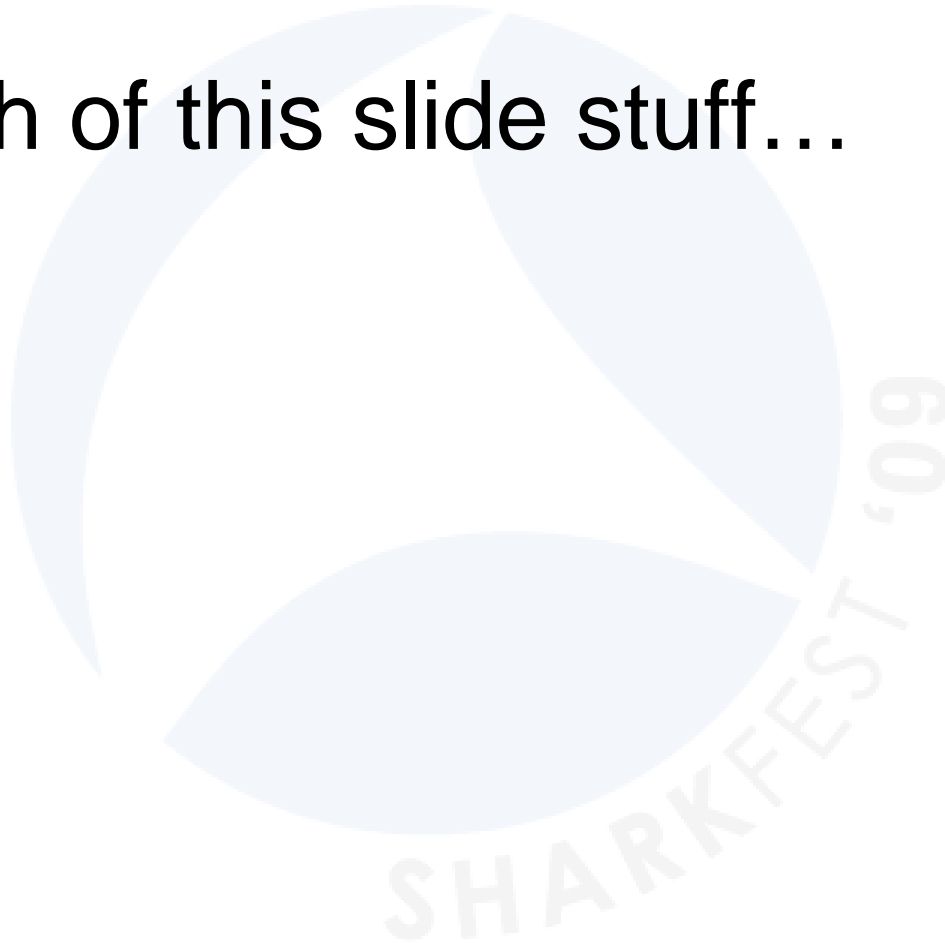
- Sequence number: 0 (relative sequence number)
- Header length: 40 bytes
- Flags: 0x2b (FIN, SYN, PSH, URG)
- Window size: 4096
- Checksum: 0x54c2 [correct]
- Urgent pointer: 0
- Options: (20 bytes)
  - Window scale: 10 (multiply by 1024)
  - NOP
  - Maximum segment size: 265 bytes

Below the packet details, there is a hex dump and ASCII representation of the packet data.

**Check out...**  
**Statistics > Protocol Hierarchies**  
**Statistics > Conversations**  
**Filter on DNS**  
**Filter on ICMP**

# Now...

- Enough of this slide stuff...



# Links

- High Technology Crime Investigation Association  
<http://www.htcia.org>
- Snooping Dragon Report  
<http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf>
- Hacked Hosts: Network Forensics  
<http://www.chappellseminars.com>
- Trace Files – Laura’s Media Roll  
<http://www.chappellseminars.com>
- AirPcap Adapters  
<http://www.cacotech.com>