

Download Laura's Trace Files at www.wiresharktraining.com/sharkfest09

Network Forensics: Wireshark as Evidence Collector

Laura Chappell

Founder, Wireshark University

<http://www.wiresharktraining.com> | laura@wiresharktraining.com

Presenter, Wireshark Jumpstart Series

<http://www.chappellseminars.com> | laura@chappellseminars.com

SHARKFEST '09

Stanford University

June 15th, 2009 10:45-12:15

Wireshark
is divine!



The OHHDL Case

Subject: Kalon Tripa Succession
From: "Pema Rinzin" <prinzintibet@yahoo.com>
Date: Thu, September 18, 2008 8:14 am
To: 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



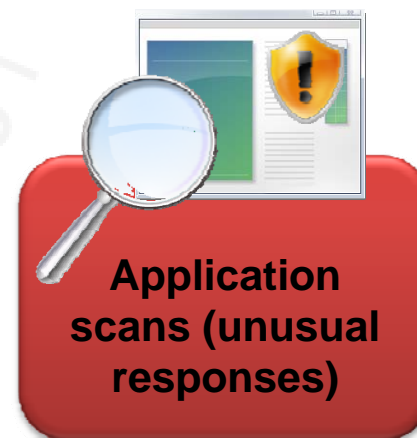
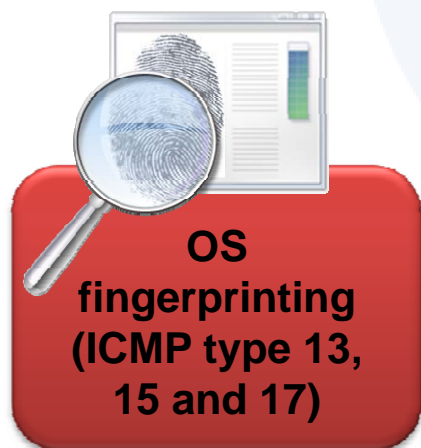
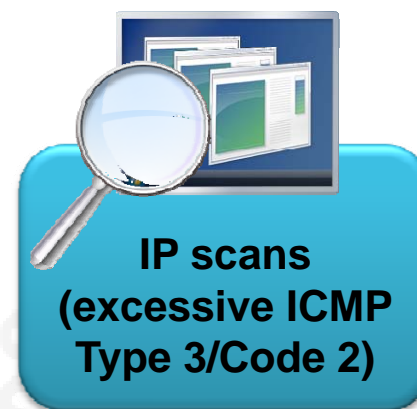
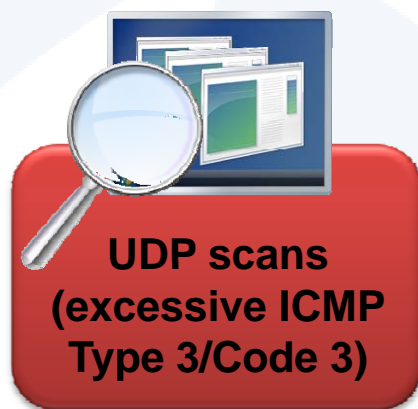
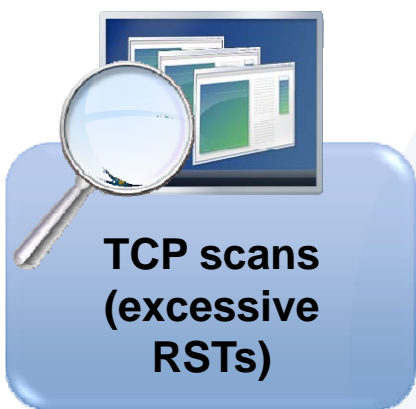
Here's your sense of false security... Enjoy your stay.

Thank goodness they have WEP on this WLAN!

In this Session

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

Evidence of Reconnaissance



Evidence of Breaches

! Unusual communication pairs

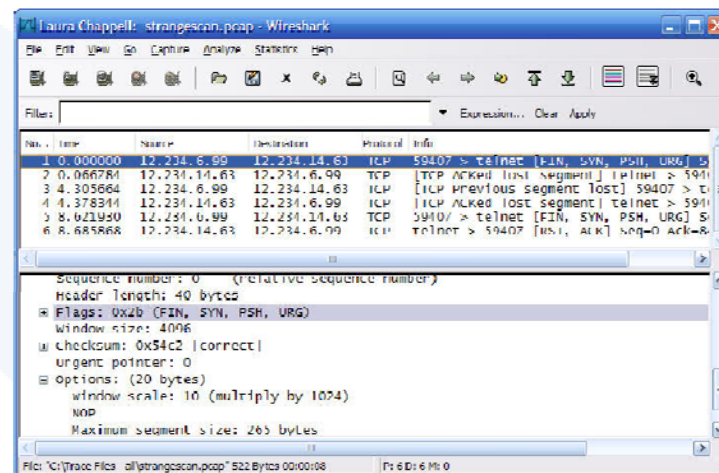
! Unusual protocols and ports

! Excessive failed connections

! Unusual inbound connections

! Unusual outbound connections

! Peer-to-peer traffic paths



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/s-hackedhosts.html>
- Yes – I tweet – “laurachappell”
- Yes – I blog - feeds2.feedburner.com/InsideLaurasLab
- Yes – I Facebook – “laurachappell”

Thank You!

- Please sign up for the Wireshark Jumpstart courses at chappellseminars.com!