threat landscape gardening

A field guide to examining discrete technology solutions

Neal Wise - Assurance Pty Ltd

Neal Wise - y Ø 11

@y Ø 11 = UNIX guy, mac security zealot, packet monkey, biz guy

@assurance

ASSURANCE

Agenda

Talk is about a process not findings

Reaalllly vague but I think I'm going somewhere with this

Taking what you know about organised technology to infer hidden components

Also I like taking pictures of busted technology

Discrete Solutions

Yeah. So I made this term up

Focused-purpose solutions that are generally isolated from other solutions (but not always)

Variously connected but many are IP networked or network accessible eventually

Examples I like

CCTV systems

A/D Telephony & VOIP

WiFi

Proximity card access systems, lifts, etc.

advertising systems & notice boards

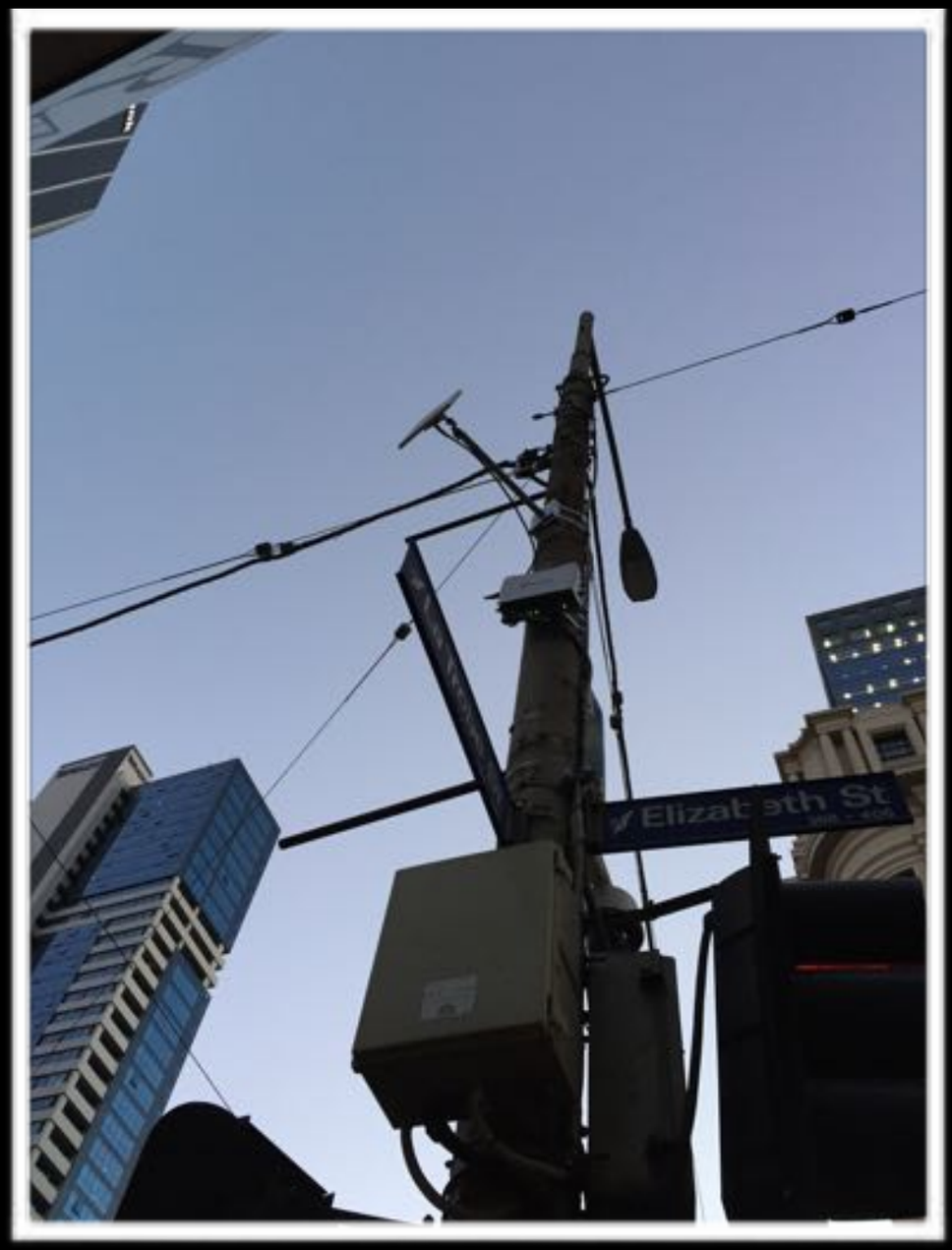
Traffic and transport

Hotel entertainment systems

In flight entertainment systems and data

so many cameras…

so many cameras…



Two endpoints of a point-to-point wireless solution for CCTV in City of Melbourne

ASSURANCE

Disclosure by observation

SNP Security

Firetide Mesh Routers

Disclosure by Case Study

Similar solution in City of Maribyrnong's Footscray CCTV solution

ASSURANCE

Disclosure by Case Study

FireTide mesh wireless. The work in the field is exemplary. With this much gear, you could excuse a bit of untidiness but the SNP boys have done extremely well in Footscray.

Better angled pics than mine

Visual ID of solution components.

Note the explanation for their technology's ugly urban blight

ASSURANCE

Disclosure by Case Study

"However, Police IT are currently investigating the creation of an email gateway to enable images to be emailed from within our network, creating an electronic audit trail, and reducing the need for copying to CD or USB."

This really seems like a bad idea

ASSURANCE

Disclosure by Case Study

wireless mesh is performing extremely well in this system.

"In fact, the original design had a fibre backbone running down to Leeds St and over the railway line but because a major State Government project involves partial demolition of the bridge over which our fibre would have run and the introduction of a whole new railway line we chose to wait."

Really, really unnecessary detail

ASSURANCE

Disclosure by creepy vendor YouTube vid

https://www.youtube.com/watch?v=584fJITv-Qw

Firetide to Help Prevent Crime in Central Footscray

firetideinc

Subscribe 158

284 views

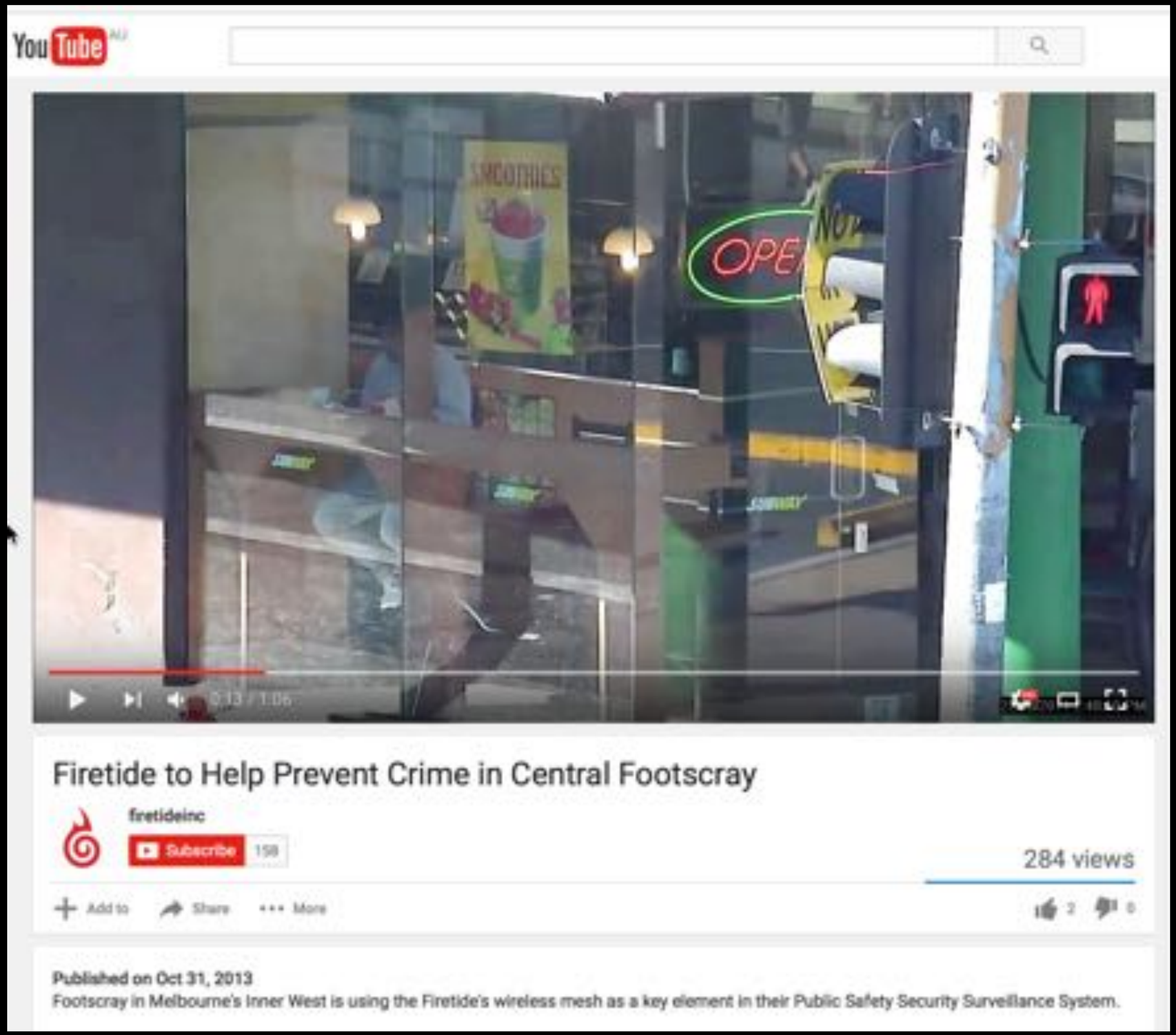
Add to Share More

Published on Oct 31, 2013

Vendor solution enthusiasm gone wrong.

ASSURANCE

Show how well the zoom works, creeps



This video has several examples of zooming the system in on the public.

Who thought this was a good idea to put on YouTube?

How isn't this a violation of the public's privacy?

ASSURANCE

It is impressive (but creepy)

Firetide to Help Prevent Crime in Central Footscray

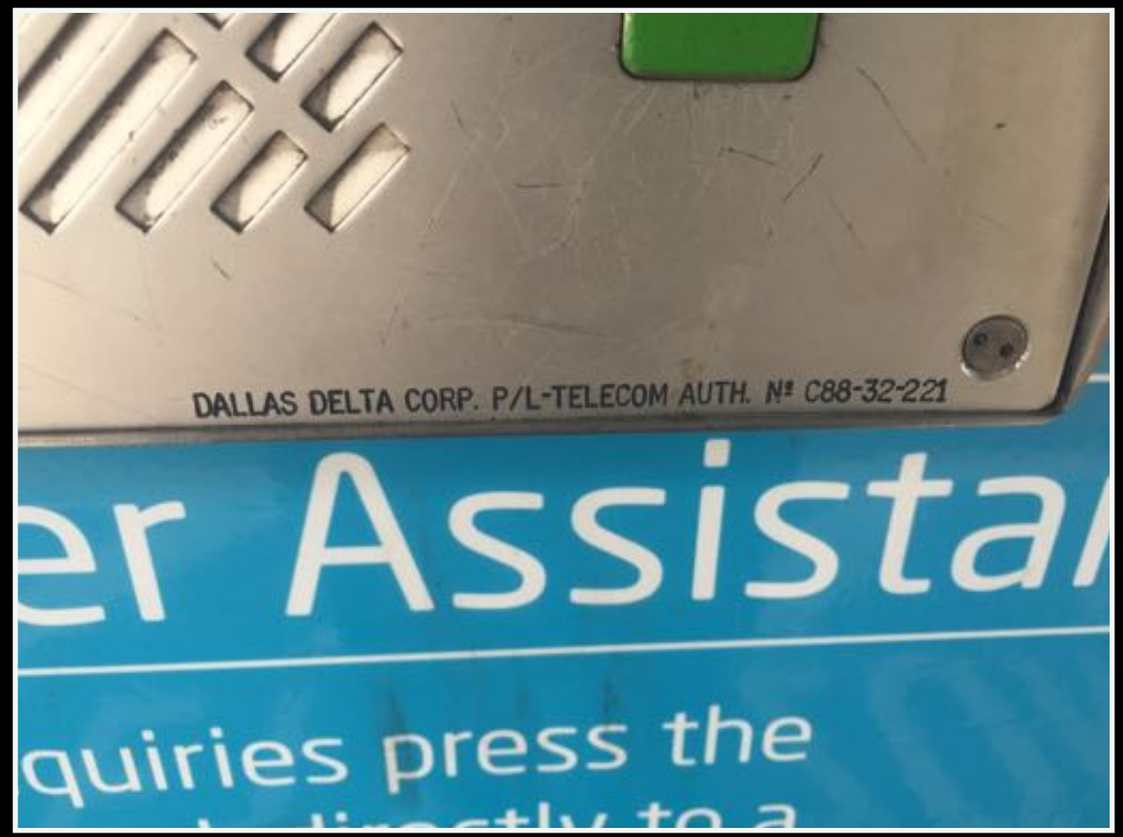
firetideinc

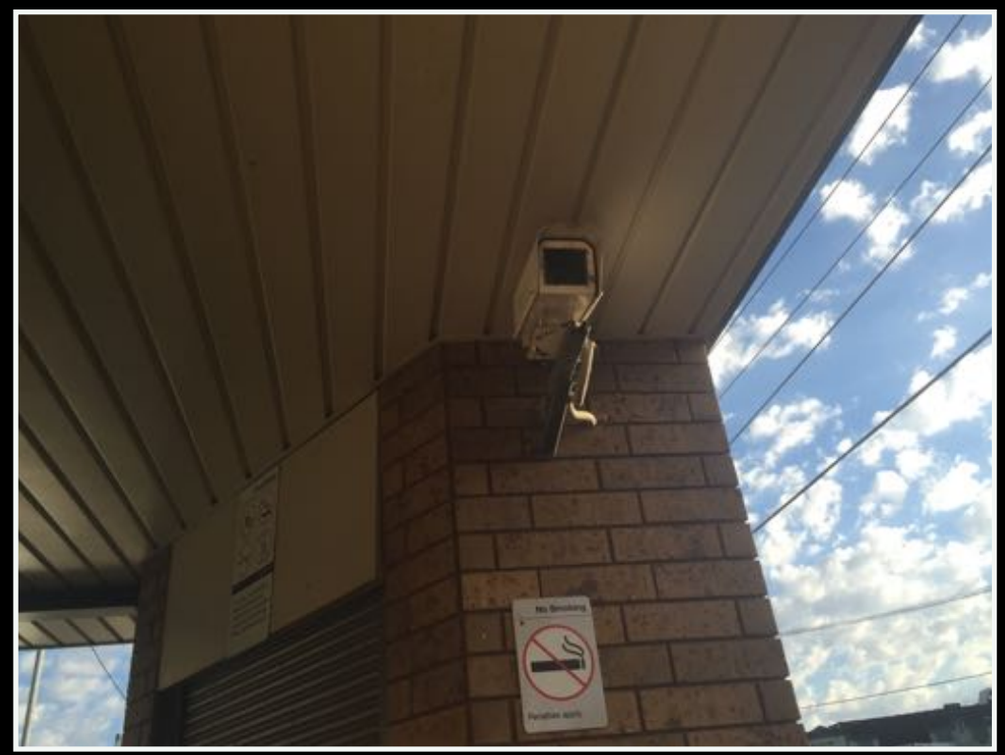
Subscribe 158

284 views

Add to Share ••• More

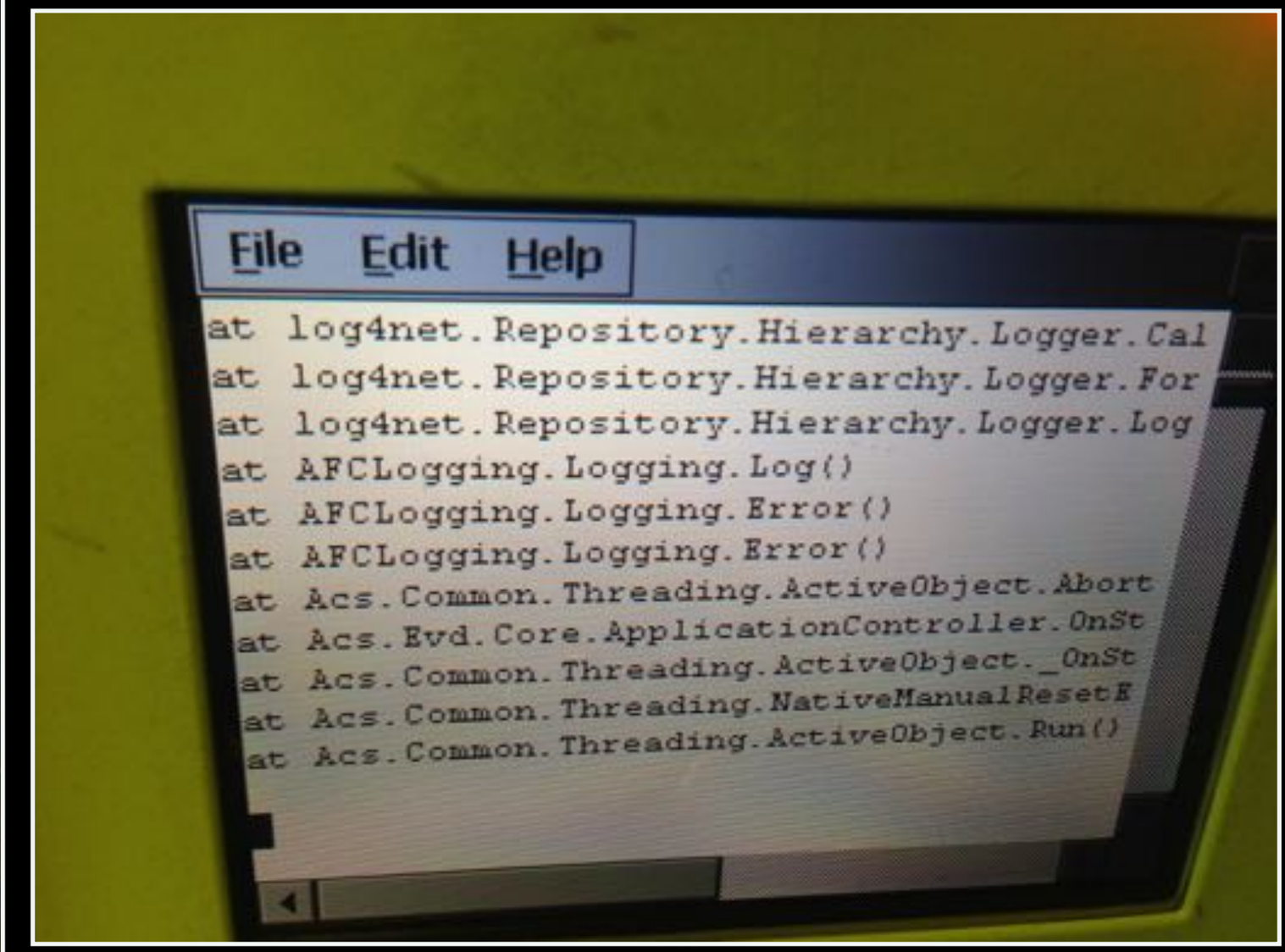
Transport stuff…





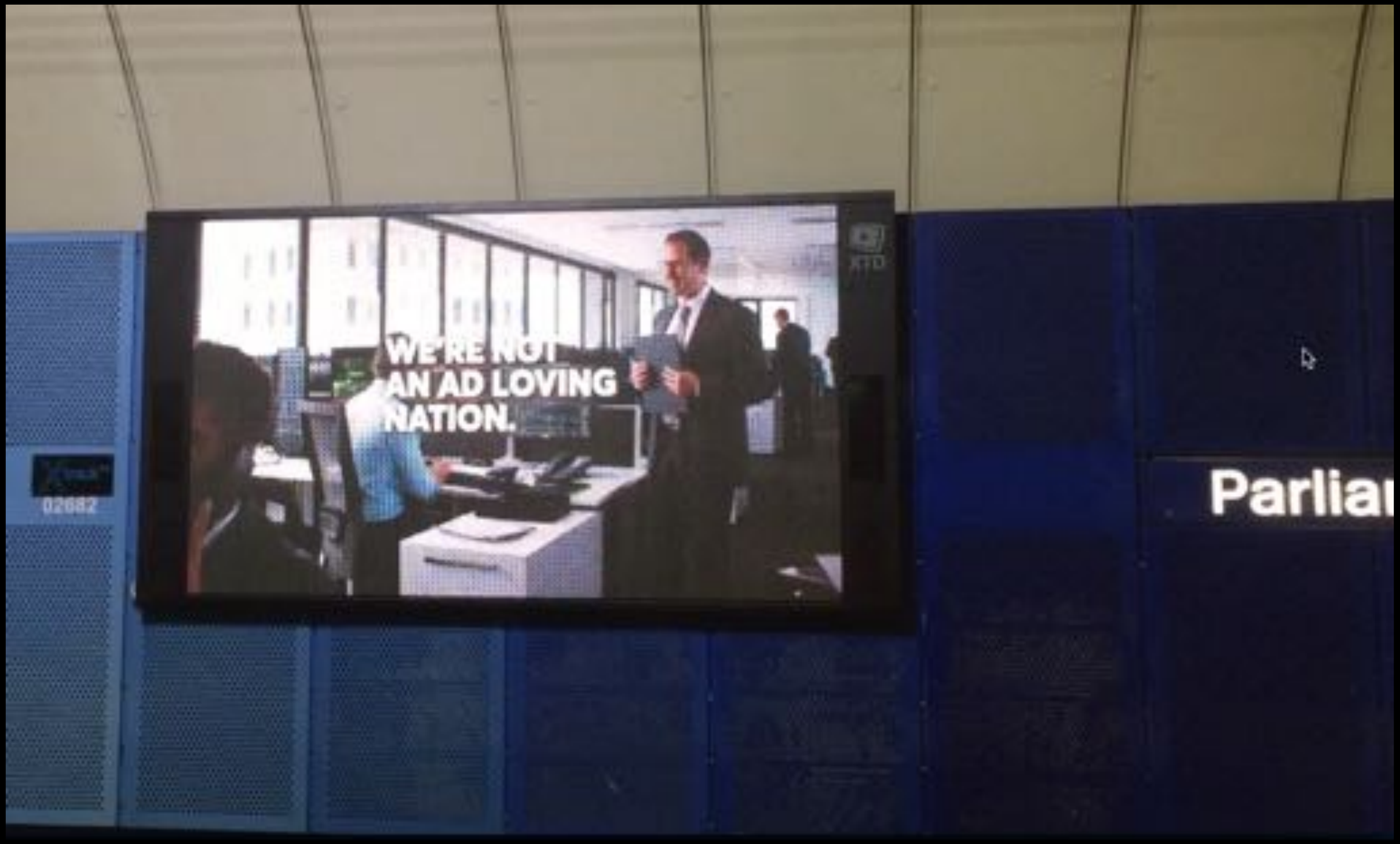
ASSURANCE

Transport stuff… myki

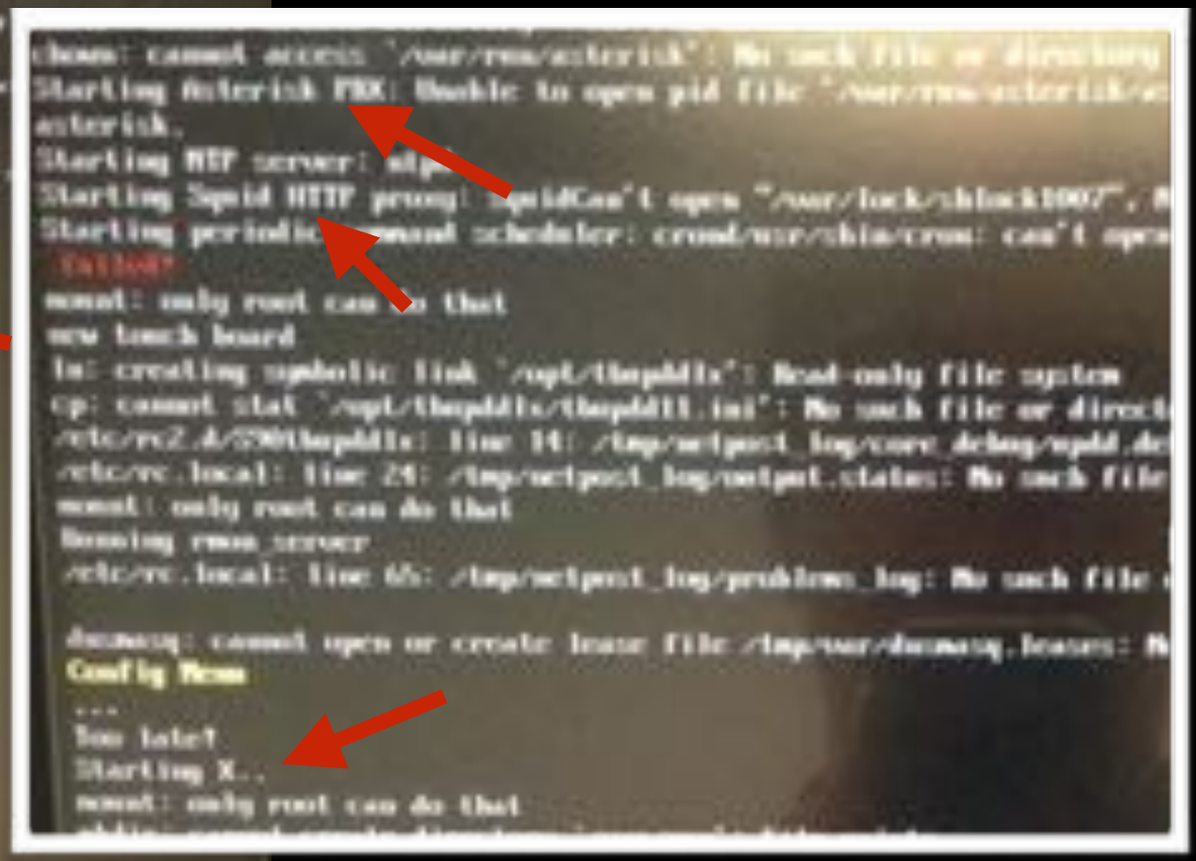


ASSURANCE

Transport stuff in Melb



Those PIE terminal things in airports



Neat… Asterisk? Squid?
X11?
Everything screaming
because of read-only
filesystem

This one recently disappeared

TRS-80 Model 100 used by City of Hobart to show tidal activity

visualising these things

Take the known to infer the unknown

Inductive reasoning?

Use what I think of as “hacker’s intuition” plus every bit of information you can grab

Take parts you can observe + your experience to prove your **threat premise**

How I look at these

more accessible ← → less accessible

audience

?

controls?

accessible services / devices

?

controls

service data

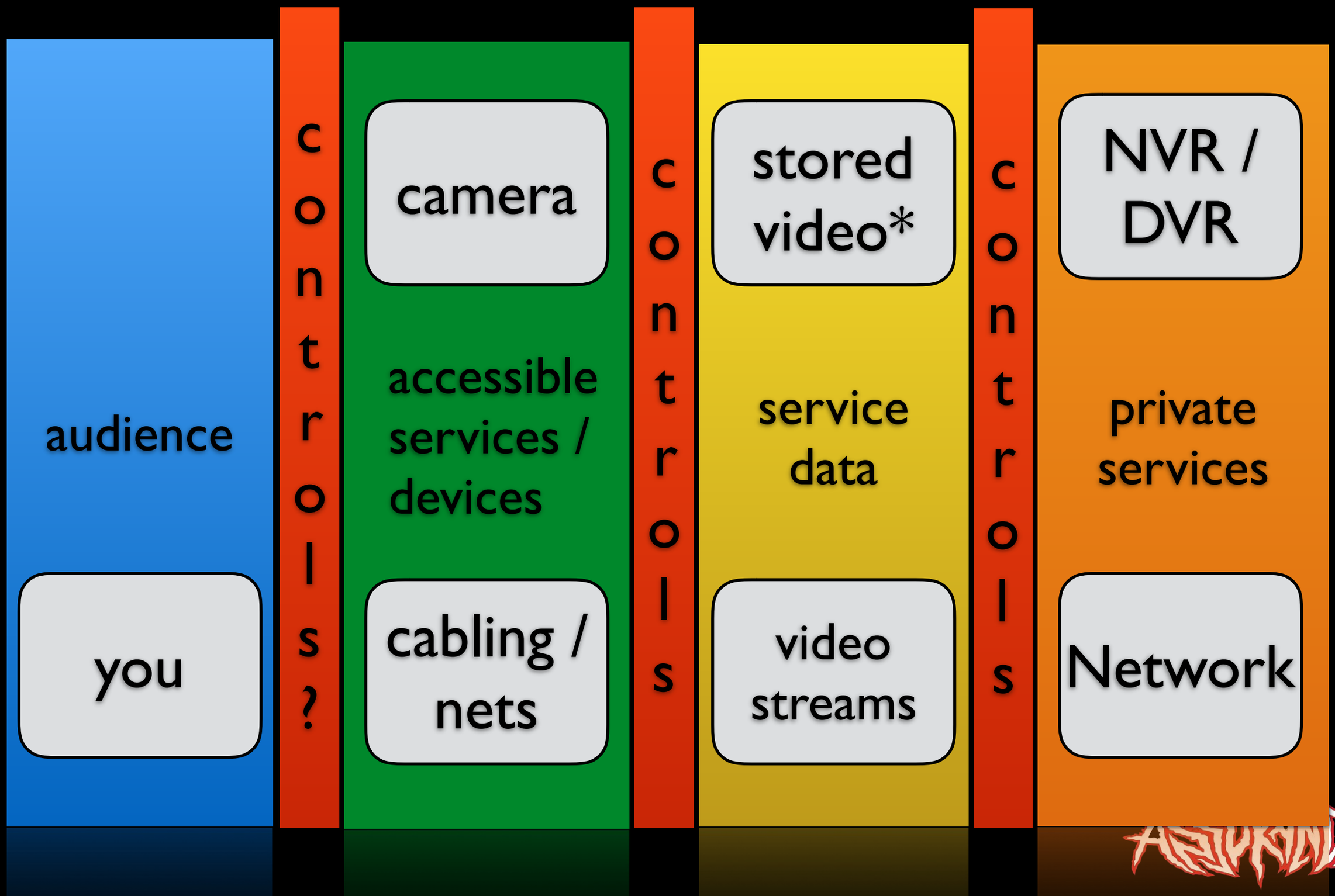
?

controls

private services

?

CCTV


audience
you
controls?
accessible services / devices
cabling / nets
controls
service data
video streams
controls
private services
Network
camera
stored video*
NVR / DVR

802.11

audience

public / private

controls?

WAP

accessible services / devices

network

controls

L2/L3 Networks

service data

L2/L3 tunnels CAPWAP

controls

mgmt services

private services

Network

VOIP

audience

physical access

control?

Phones / Video Conferencing

accessible services / devices

L2 / L3 Networks

control

"plumbing" DHCP / TFTP etc

service data

SIP / H.323 / RTSP / etc.

control

SIP/ Proxy

private services

Gateway Gatekeeper / PSTN

Opportunistic attack

Applying this thinking to accessible technology in the course of looking at your life / job / whatever critically

obvious process

Visual observation to collect identifiable details
=> “research”

Passive connection to target to ^^^
=> “research”

Active connection to target to ^^^
=> “research”

toys

Opportunity	Accessible device
Motive	Not enough coffee
Means	Toys like Dualcomm Ethernet “tap” (it’s not exactly a tap); UBNT USB wifi; HackRF

Demo: passive recon on a VoIP solution using a mirror tap

"Passive" port mirror tap using a Dualcomm

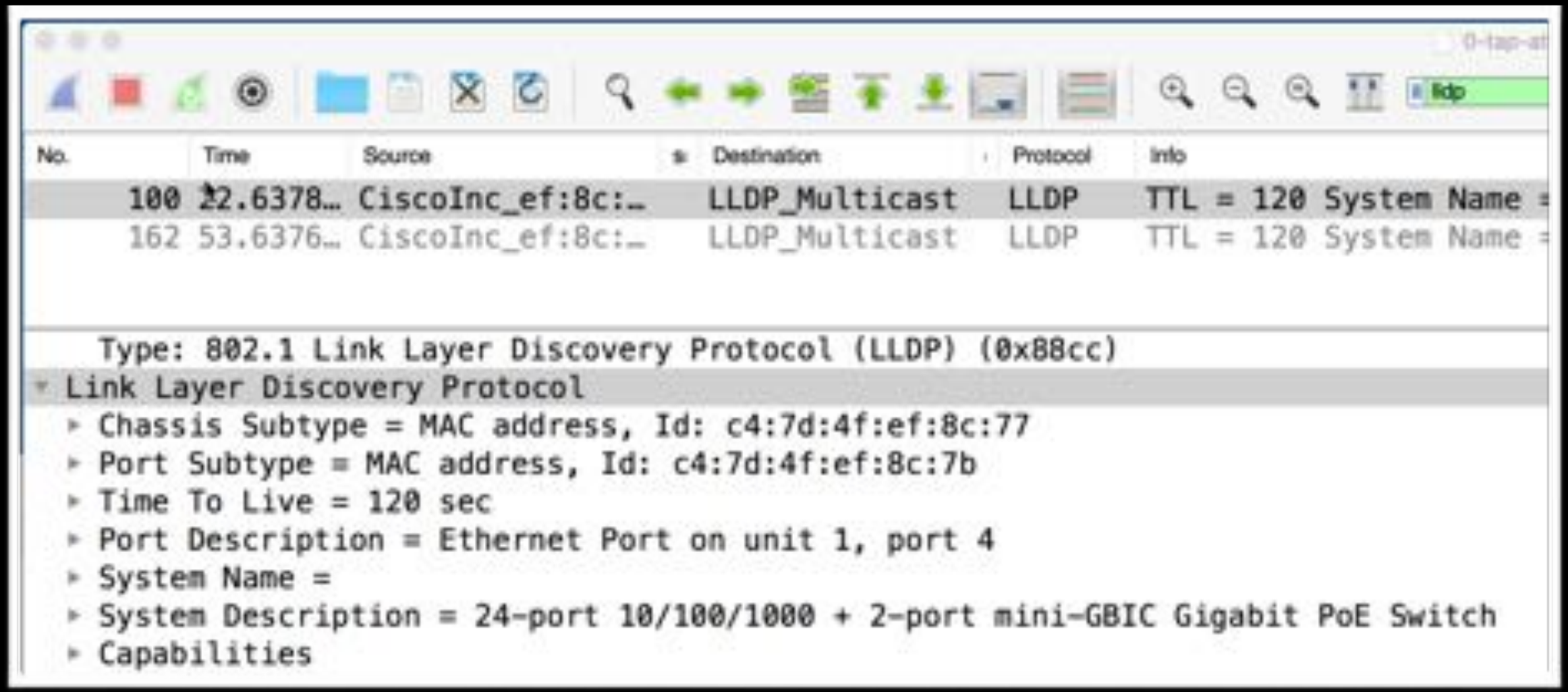
Pass through 802.3af Power over Ethernet from port 1 to port 2

"Mirror" port 1/2 to port 5 for sniffing

Wireshark on an interface configured to not request a DHCP address

ASSURANCE

CDP/LLDP


lldp
No. Time Source Destination Protocol Info
100 22.6378… CiscoInc_ef:8c:… LLDP_Multicast LLDP TTL = 120 System Name =
162 53.6376… CiscoInc_ef:8c:… LLDP_Multicast LLDP TTL = 120 System Name =
Type: 802.1 Link Layer Discovery Protocol (LLDP) (0x88cc)
Link Layer Discovery Protocol
Chassis Subtype = MAC address, Id: c4:7d:4f:ef:8c:77
Port Subtype = MAC address, Id: c4:7d:4f:ef:8c:7b
Time To Live = 120 sec
Port Description = Ethernet Port on unit 1, port 4
System Name =
System Description = 24-port 10/100/1000 + 2-port mini-GBIC Gigabit PoE Switch
Capabilities

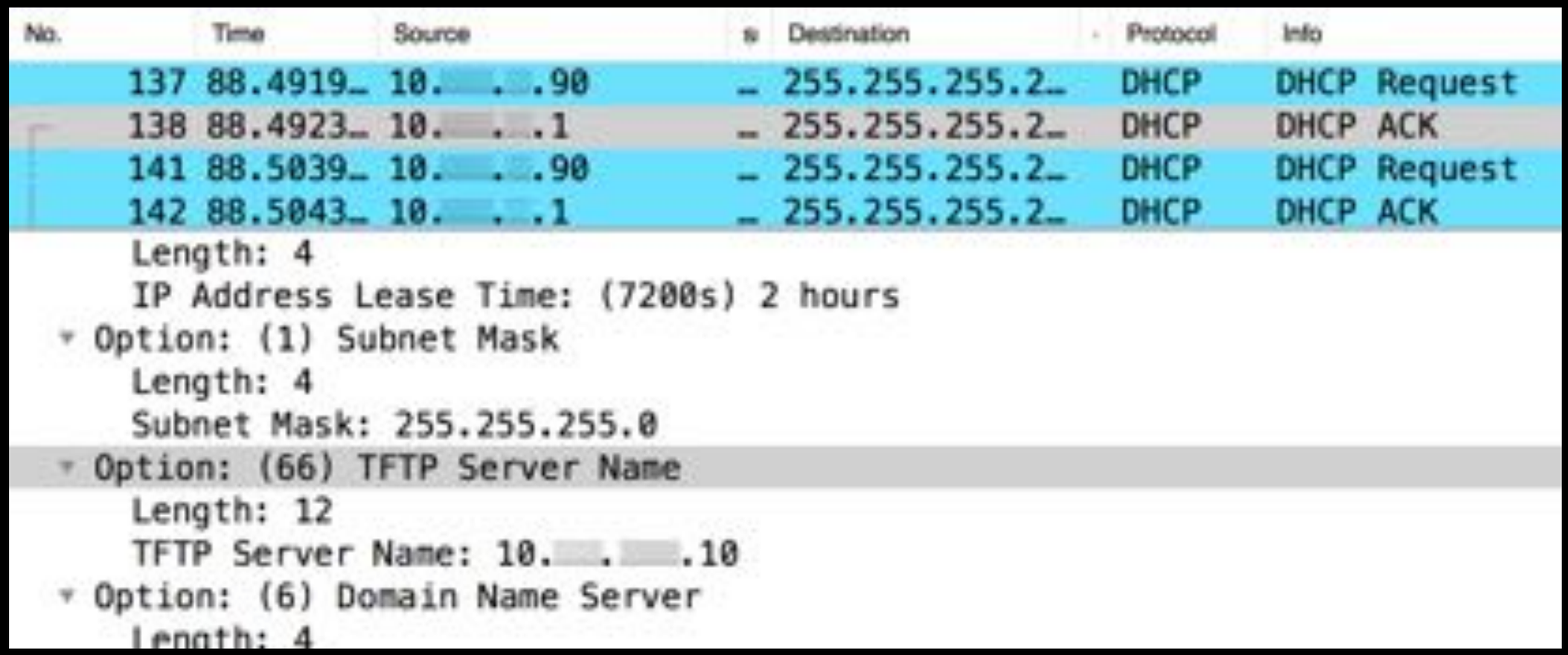
CDP/LLDP

```
▾ Management Address
    0001 000. .... .... = TLV Type: Management Address (8)
    .... ...0 0000 1100 = TLV Length: 12
    Address String Length: 5
    Address Subtype: IPv4 (1)
    Management Address: 10.   .  .5
    Interface Subtype: ifIndex (2)
    Interface Number: 1001
    OID String Length: 0
```

management IP address

likely in same L3 network available at port

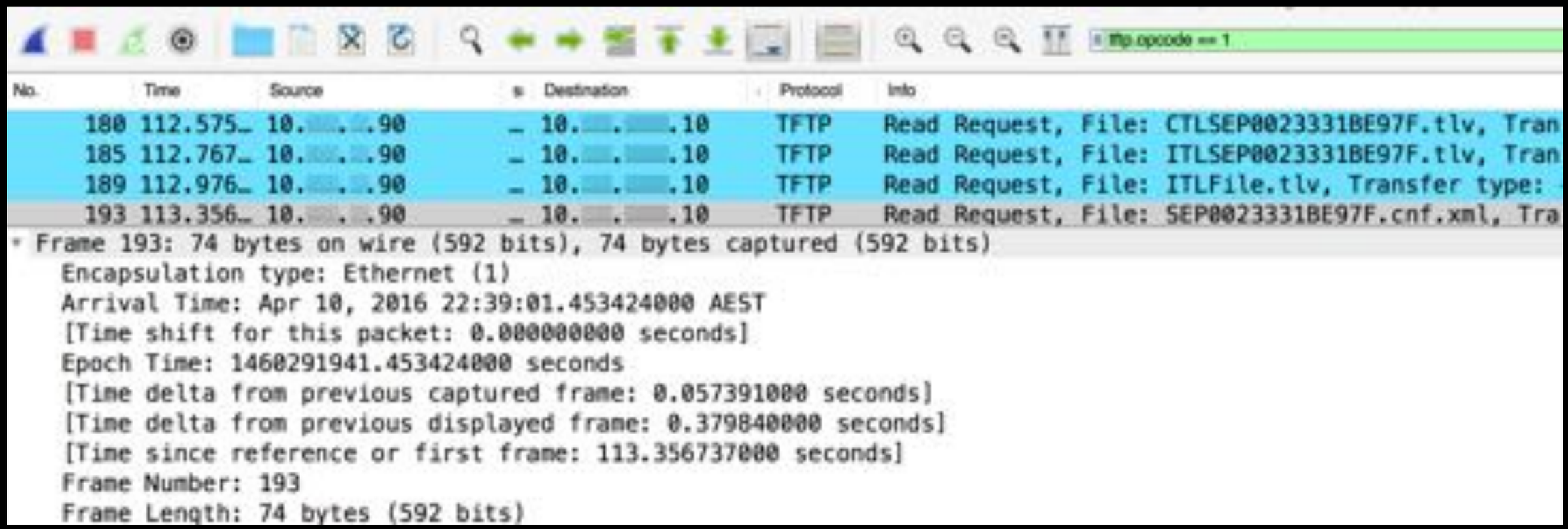
DHCP options



TFTP server specified by DHCP

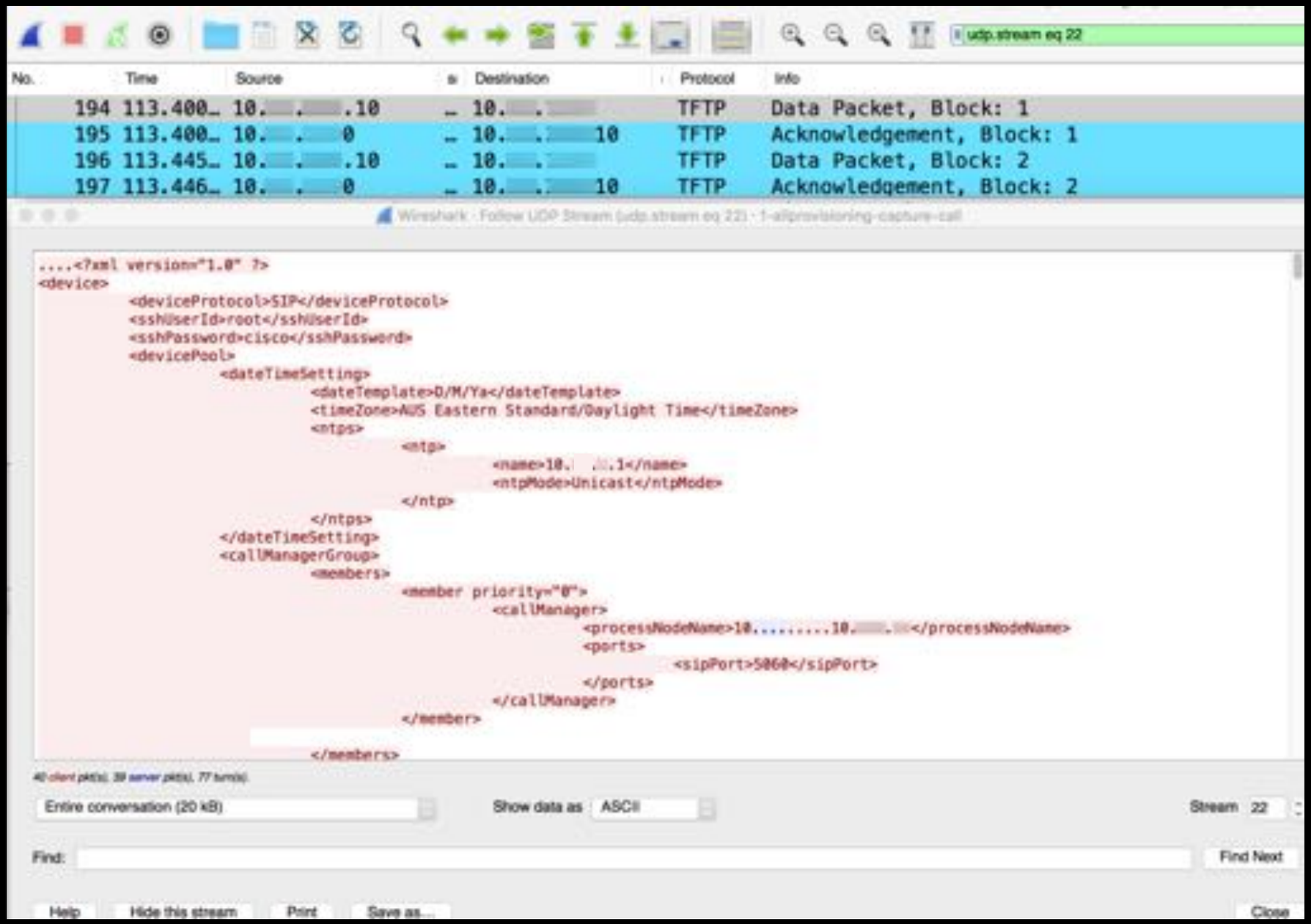
- common for phone, camera provisioning
- May also be SIP server

TFTP provisioning



TFTP server “Read Request”
-wireshark display tftp.opcode == 1

Passive TFTP collection



Phone configuration via TFTP confirms SIP server IP

Passive TFTP collection

```
<line button="1" lineIndex="1">
        <featureID>9</featureID>
        <featureLabel>Extension: 708</featureLabel>
        <proxy>USECALLMANAGER</proxy>
        <port>5060</port>
        <name>    </name>
        <authName>    </authName>
        <authPassword>                </authPassword>
        <messageWaitingLampPolicy>3</messageWaitingLampPolicy>
        <messagesNumber>*97</messagesNumber>
        <displayName></displayName>
        <contact></contact>
        <autoAnswer>
                <autoAnswerEnabled>2</autoAnswerEnabled>
</autoAnswer>
<featureOptionMask>1</featureOptionMask>
<callWaiting>3</callWaiting>
<sharedLine>false</sharedLine>
<messageWaitingAMWI>1</messageWaitingAMWI>
<ringSettingIdle>4</ringSettingIdle>
<ringSettingActive>5</ringSettingActive>
<forwardCallInfoDisplay>
                        <callerName>true</callerName>
                <callerNumber>false</callerNumber>
                <redirectedNumber>false</redirectedNumber>
<dialedNumber>true</dialedNumber>
```

SIP server registration details

mitigations

Monitor network-connected device presence - if things reboot, disappear/reappear find the root cause

For devices<==>services mutual auth with strong transport encryption but know its limitations - 802.1x/NAC, Locally Significant Certificates / TLS for SRTP/ZRTP, etc.

Where possible apply “port security” or MAC- filter controls to only permit known L2 devices. These are defeat-able but help

Thanks BSides

web:
www.assurance.com.au

twitters:
@assurance @y0l1