Digital Forensics
Lecture Week 4

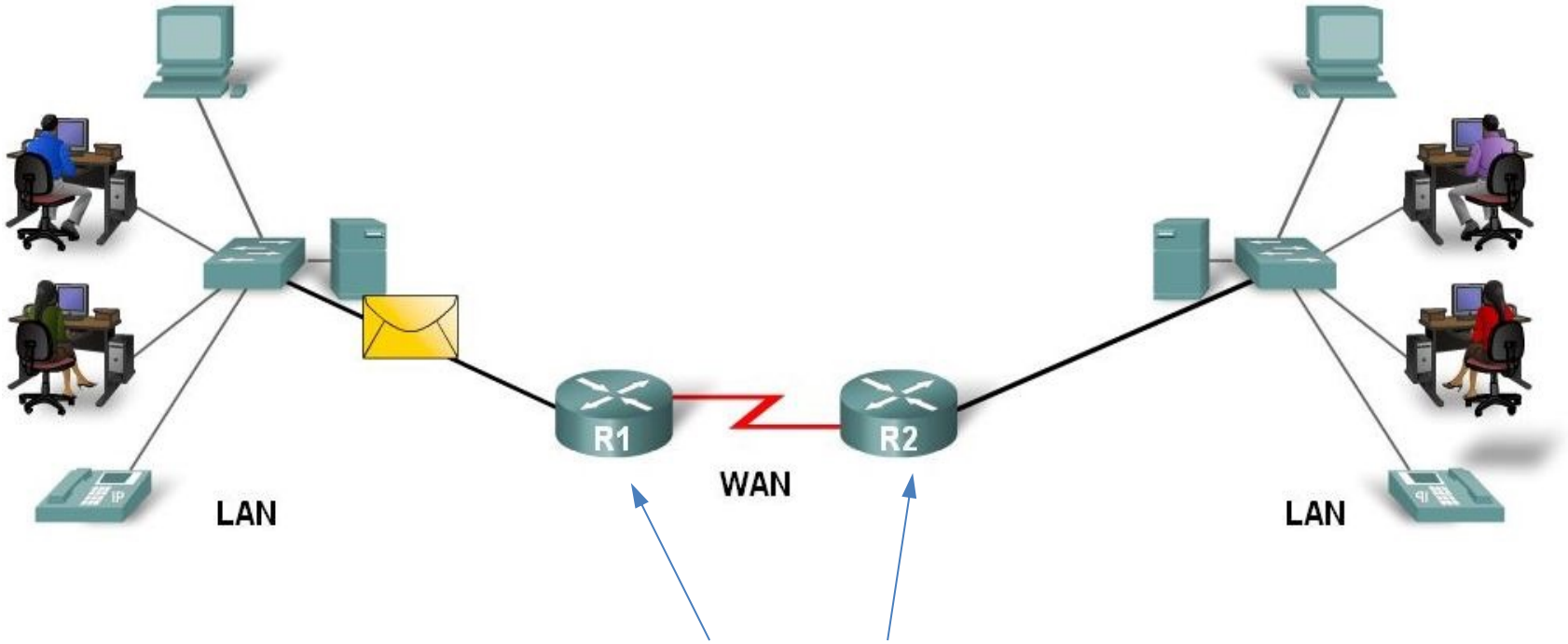
# Network Based Evidence
# Packet Captures

Readings
Nelson - Ch10

# Objectives

- To understand network abuse/attack basics
- To classify methods of collecting network evidence
- To revise the features of Wireshark
- To use packet captures to **baseline** network activity

# The Network




- All Internet packets are available  at the edge router

# Network Abuse

- A suspect downloads prohibited images
- A disk examination may not find evidence of this
- He may store on USB so avoids detection on work PC
- A suspect may conduct a private business on work PC
- He may avoid raising suspicions
- A suspect may access sensitive company data and exfiltrate it to a remote internet location
- Network forensic examiners identify unusual network traffic

# Network Attacks

- Is a rise in traffic innocent or an attack?
- Intrusions into a network leave a trail
  - In the network firewall
  - In the network Intrusion Detection System (IDS)
  - In the network proxy server
- Network forensic examiners identify compromised machines and take them offline

# Network Defences

- As discussed in the old Network Security subject we use defence in depth
- Internet facing firewall and IDS
- Demilitarised Zone (DMZ) network bridge
- LAN facing firewall and IDS
- Firewall and Antivirus on the hosts

# Defence modes

- People
  - you need well trained people dedicated to defending the network
- Technology
  - a strong network architecture, proven IDSs and firewalls
  - penetration testing
  - systems for log analysis
- Operations
  - updating security patches
  - training and monitoring users
  - disaster recovery plans

# Network Activity protocols

- Device Startup
  - dhcp
- Device connection
  - ssh or telnet
- Background noise
  - Switch STP
  - Routing protocols (OSPF)
  - Windows AD
- User activity
  - access a Website
  - send/receive email
  - access a work connection (VPN)
- Intruder Activity
  - as above
  - also use a back door

# Network Based Forensics

- An attack on a Digital Device can be performed in person or over the digital network
- We will look at in person attacks later
- A network attack involves:
- Opening a trapdoor on the target device
- Contacting the target device from a remote device
- Exchanging network packets to:
- Install snooping software
- then retrieve sensitive information such as passwords

# Network Intrusion Detection

- We can detect intrusion in several ways:
- Use a special Intrusion Detection hardware - IDS/IPS
- Equip a firewall with IDS features
- Have a Network based IDS examine all network packets
- Have a Host based IDS examine local network activity
- Record network activity in local log files
- Use a local Firewall/Virus Scanner

# Locating the evidence

- Network evidence can be found:
- On a suspect's device
  - file folders, cache folders and swap files
- On the local network
  - proxies, firewalls, IDS
- On the ISP
  - proxies, firewalls
- On the remote web site
  - logs

# Missing Evidence

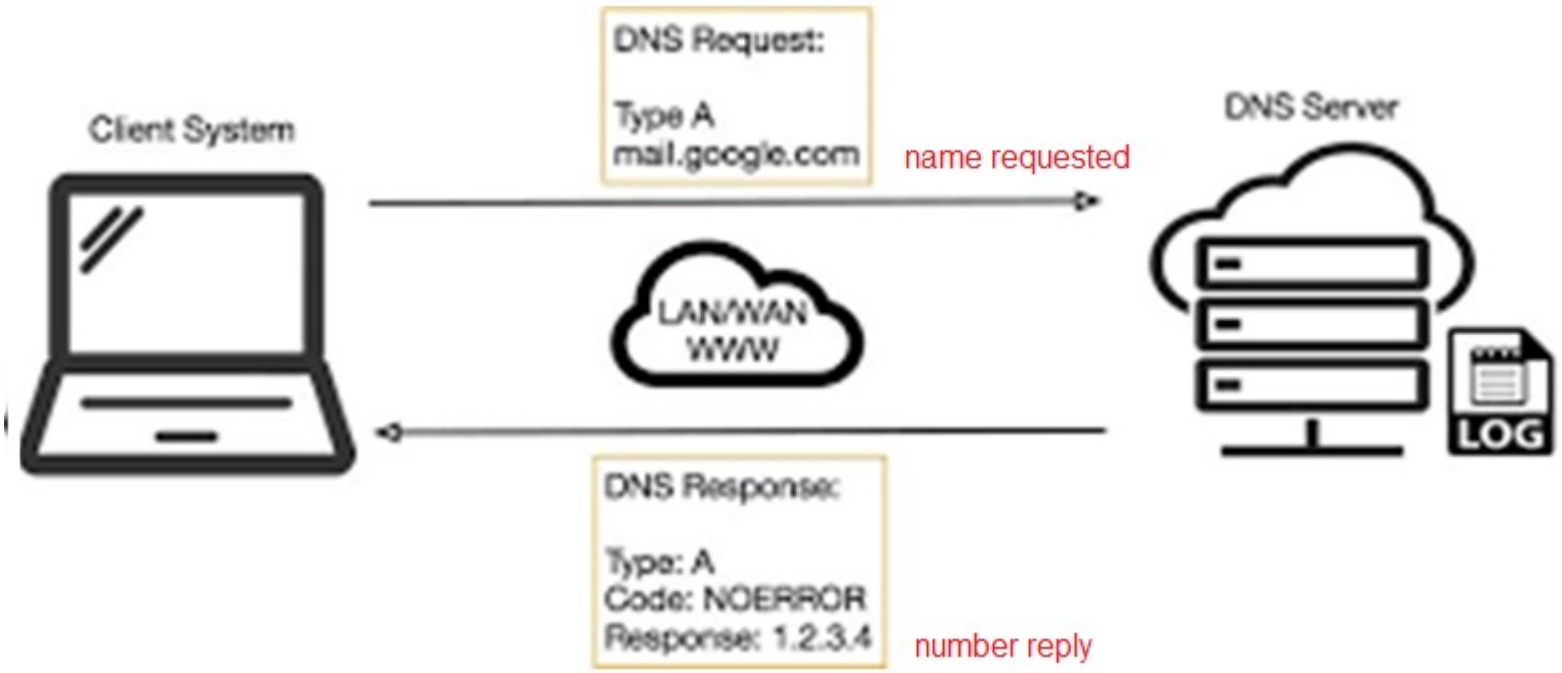
- If a browser is setup to not save third party cookies
- There will be no third party cookies on disk
- However the cookies are still sent by the server
- A network packet capture will catch the cookies
- However packet capture is resource intensive
- You need to be suspicious before collecting packets

# Accessing a Website - sequence

- dns request
- http handshake
  - browser details
  - server details
- html handshake
  - style sheets
  - JavaScript
- page display
  - images, gifs and pngs
- SSL
  - SSL certificate exchange
- plug-ins
  - flash
- extras
  - cookies
  - hit counters
  - page tracking
  - ASP.Net

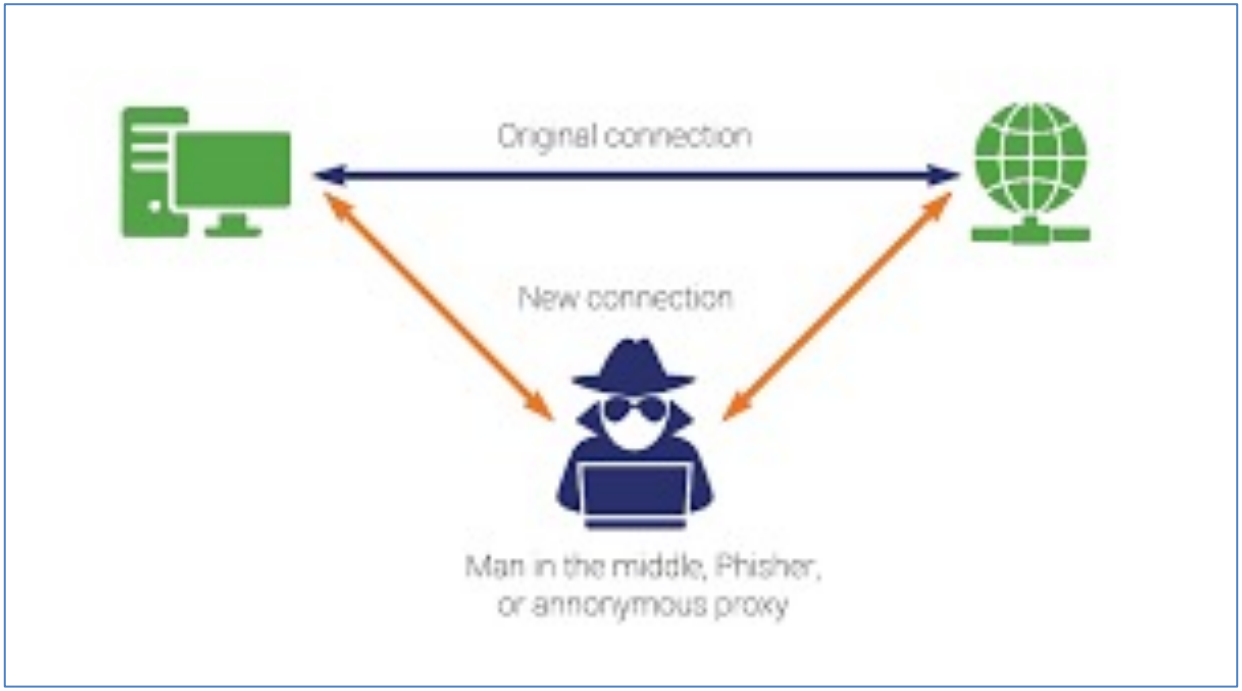
# DNS #1

- Resolves the name of the target website to an IP address.



# DNS #2

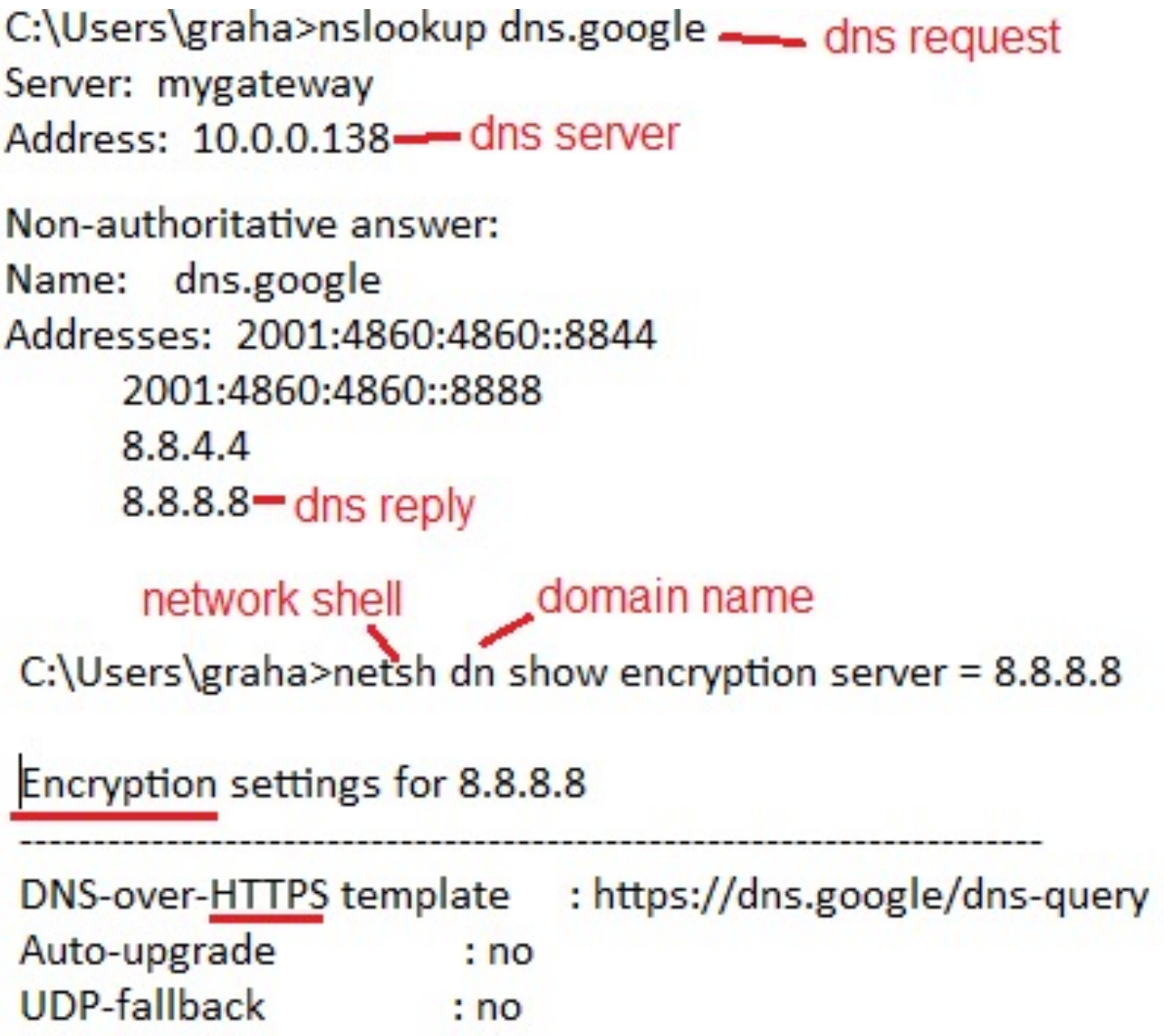
- Subject to hacking by a man in the middle attack
- Reveals dns request/reply to wireshark




- More secure encrypted dns is coming into use.

# Secure dns using the DoH client

(dns over https)



# Text on the Internet

- There are several ways text data can be saved in a database.
  - A list of Plaintext as txt files, each item is separated by a space or a TAB
  - A list of Comma separated Variables as csv files, each item is separated by a comma (,)
  - A list of JavaScript Object Notation (JSON) files, each item is named with quotes (“) and separated by a comma (, )
    - "country_id":"AU","city":"Chatswood"

# Ascii encoding

| Dec | Hex | Oct | Chr | Dec | Hex | Oct | HTML | Chr | Dec | Hex | Oct | HTML | Chr | Dec | Hex | Oct | HTML | Chr |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 000 | NULL | 32 | 20 | 040 | &#032; | Space | 64 | 40 | 100 | &#064; | @ | 96 | 60 | 140 | &#096; | ` |
| 1 | 1 | 001 | Start of Header | 33 | 21 | 041 | &#033; | ! | 65 | 41 | 101 | &#065; | A | 97 | 61 | 141 | &#097; | a |
| 2 | 2 | 002 | Start of Text | 34 | 22 | 042 | &#034; | " | 66 | 42 | 102 | &#066; | B | 98 | 62 | 142 | &#098; | b |
| 3 | 3 | 003 | End of Text | 35 | 23 | 043 | &#035; | # | 67 | 43 | 103 | &#067; | C | 99 | 63 | 143 | &#099; | c |
| 4 | 4 | 004 | End of Transmission | 36 | 24 | 044 | &#036; | $ | 68 | 44 | 104 | &#068; | D | 100 | 64 | 144 | &#100; | d |
| 5 | 5 | 005 | Enquiry | 37 | 25 | 045 | &#037; | % | 69 | 45 | 105 | &#069; | E | 101 | 65 | 145 | &#101; | e |
| 6 | 6 | 006 | Acknowledgment | 38 | 26 | 046 | &#038; | & | 70 | 46 | 106 | &#070; | F | 102 | 66 | 146 | &#102; | f |
| 7 | 7 | 007 | Bell | 39 | 27 | 047 | &#039; | ' | 71 | 47 | 107 | &#071; | G | 103 | 67 | 147 | &#103; | g |
| 8 | 8 | 010 | Backspace | 40 | 28 | 050 | &#040; | ( | 72 | 48 | 110 | &#072; | H | 104 | 68 | 150 | &#104; | h |
| 9 | 9 | 011 | Horizontal Tab | 41 | 29 | 051 | &#041; | ) | 73 | 49 | 111 | &#073; | I | 105 | 69 | 151 | &#105; | i |
| 10 | A | 012 | Line feed | 42 | 2A | 052 | &#042; | * | 74 | 4A | 112 | &#074; | J | 106 | 6A | 152 | &#106; | j |
| 11 | B | 013 | Vertical Tab | 43 | 2B | 053 | &#043; | + | 75 | 4B | 113 | &#075; | K | 107 | 6B | 153 | &#107; | k |
| 12 | C | 014 | Form feed | 44 | 2C | 054 | &#044; | , | 76 | 4C | 114 | &#076; | L | 108 | 6C | 154 | &#108; | l |
| 13 | D | 015 | Carriage return | 45 | 2D | 055 | &#045; | - | 77 | 4D | 115 | &#077; | M | 109 | 6D | 155 | &#109; | m |
| 14 | E | 016 | Shift Out | 46 | 2E | 056 | &#046; | . | 78 | 4E | 116 | &#078; | N | 110 | 6E | 156 | &#110; | n |
| 15 | F | 017 | Shift In | 47 | 2F | 057 | &#047; | / | 79 | 4F | 117 | &#079; | O | 111 | 6F | 157 | &#111; | o |
| 16 | 10 | 020 | Data Link Escape | 48 | 30 | 060 | &#048; | 0 | 80 | 50 | 120 | &#080; | P | 112 | 70 | 160 | &#112; | p |
| 17 | 11 | 021 | Device Control 1 | 49 | 31 | 061 | &#049; | 1 | 81 | 51 | 121 | &#081; | Q | 113 | 71 | 161 | &#113; | q |
| 18 | 12 | 022 | Device Control 2 | 50 | 32 | 062 | &#050; | 2 | 82 | 52 | 122 | &#082; | R | 114 | 72 | 162 | &#114; | r |
| 19 | 13 | 023 | Device Control 3 | 51 | 33 | 063 | &#051; | 3 | 83 | 53 | 123 | &#083; | S | 115 | 73 | 163 | &#115; | s |
| 20 | 14 | 024 | Device Control 4 | 52 | 34 | 064 | &#052; | 4 | 84 | 54 | 124 | &#084; | T | 116 | 74 | 164 | &#116; | t |
| 21 | 15 | 025 | Negative Ack. | 53 | 35 | 065 | &#053; | 5 | 85 | 55 | 125 | &#085; | U | 117 | 75 | 165 | &#117; | u |
| 22 | 16 | 026 | Synchronous idle | 54 | 36 | 066 | &#054; | 6 | 86 | 56 | 126 | &#086; | V | 118 | 76 | 166 | &#118; | v |
| 23 | 17 | 027 | End of Trans. Block | 55 | 37 | 067 | &#055; | 7 | 87 | 57 | 127 | &#087; | W | 119 | 77 | 167 | &#119; | w |
| 24 | 18 | 030 | Cancel | 56 | 38 | 070 | &#056; | 8 | 88 | 58 | 130 | &#088; | X | 120 | 78 | 170 | &#120; | x |
| 25 | 19 | 031 | End of Medium | 57 | 39 | 071 | &#057; | 9 | 89 | 59 | 131 | &#089; | Y | 121 | 79 | 171 | &#121; | y |
| 26 | 1A | 032 | Substitute | 58 | 3A | 072 | &#058; | : | 90 | 5A | 132 | &#090; | Z | 122 | 7A | 172 | &#122; | z |
| 27 | 1B | 033 | Escape | 59 | 3B | 073 | &#059; | ; | 91 | 5B | 133 | &#091; | [ | 123 | 7B | 173 | &#123; | { |
| 28 | 1C | 034 | File Separator | 60 | 3C | 074 | &#060; | < | 92 | 5C | 134 | &#092; | \ | 124 | 7C | 174 | &#124; | \| |
| 29 | 1D | 035 | Group Separator | 61 | 3D | 075 | &#061; | = | 93 | 5D | 135 | &#093; | ] | 125 | 7D | 175 | &#125; | } |
| 30 | 1E | 036 | Record Separator | 62 | 3E | 076 | &#062; | > | 94 | 5E | 136 | &#094; | ^ | 126 | 7E | 176 | &#126; | ~ |
| 31 | 1F | 037 | Unit Separator | 63 | 3F | 077 | &#063; | ? | 95 | 5F | 137 | &#095; | _ | 127 | 7F | 177 | &#127; | Del |

asciichars.com

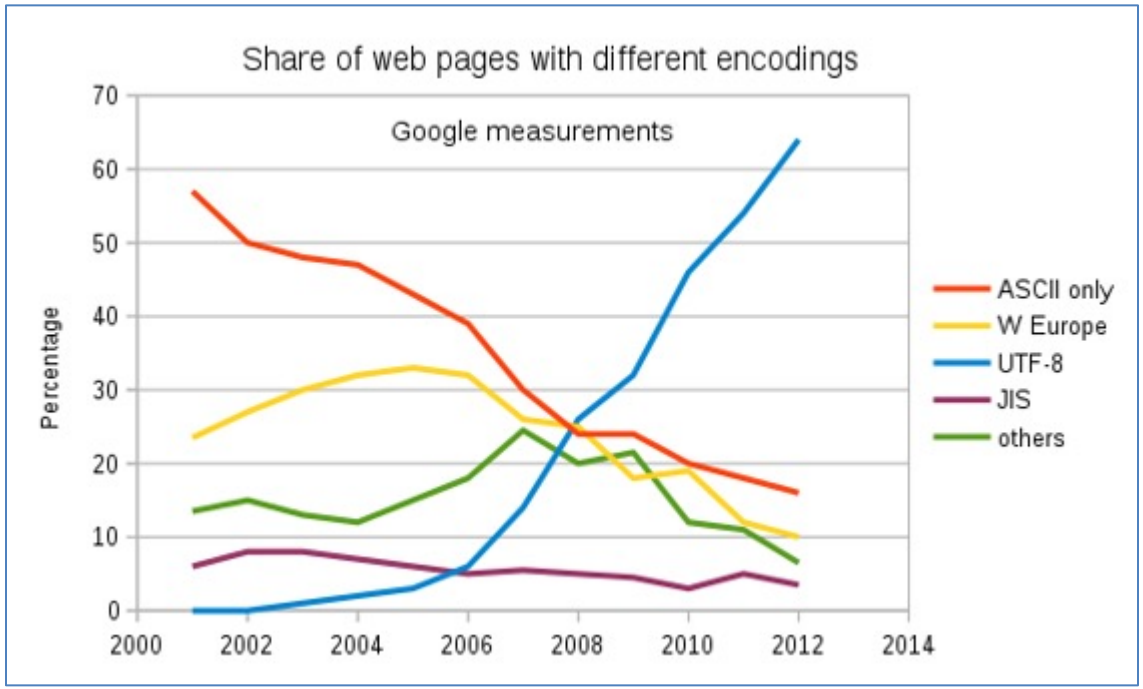
# URL Encoding

- Also called % encoding
- non alphanumeric characters  can only be sent over the Internet using the  ASCII character-set.
- For example:
- address.com/page 1/ → address.com%2Fpage%201%2F
- You will see % encoding in your captured http packets

- http://www.w3schools.com/tags/ref_urlencode.asp

# Unicode Byte Encoding

- **UTF-8**: 1-byte for the first 127 code points (maintaining compatibility with ASCII), and an optional additional 1-3 bytes (4 bytes total) for other characters




Utf-8 Usage on the Web

- 2010 → 50.6%
- 2011 → 59.8%
- 2012 → 68.0%
- 2013 → 74.7%
- 2014 → 78.7%
- 2015 → 82%
- 2016 → 87.2%
- 2017 → 88.2%
- 2018 → 90.5%
- 2019 → 92.8%

# Objectives

- To understand network abuse/attack basics
- To classify methods of collecting network evidence
- To revise the features of Wireshark
- How to use packet captures to baseline a device NBE

# Network Based Evidence - NBE

- There are four broad methods
- Full content Data
  - examine every packet
- Session Data
  - examine tcp session data
- Alert Data
  - examine errors and exceptions
- Statistical Data
  - examine unusual events

# Full Content Data

- Collect every bit of every packet.
- On Ethernet or Wireless
- Need a packet capture library (libpcap) on the device network interface
- Wireshark is a typical application
- Usually only used after an intrusion
- Extensive disk space used
- Excellent evidence
  - can detect attacks on other systems
  - can expose advanced attacks
- Encrypted packets can be a problem

# Session Data

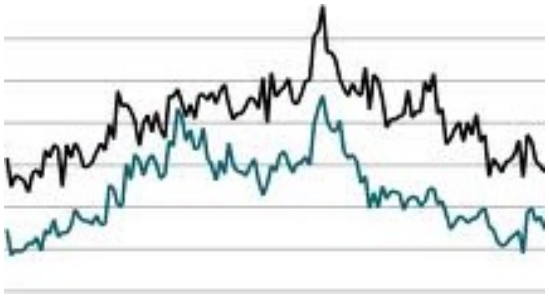
- Derived from the tcp sessions
- Often available during the initial intrusion
- Indicates time and date and parties involved
- Can often see all the intrusion sequence
- Look for strange ip addresses
- Look for unusual ports in use, for example  IRC
- High traffic could be a file transfer
- Session dns requests are not encrypted

# Alert Data

- When an IDS/IPS sees a packet that matches a virus signature or an intrusion rule, it sends an alert
- The IPS needs tuning for best results
  - avoid false positives
  - watch a back door
- Usually will not detect theft of sensitive data
- Encrypted packets can be a problem

# Statistical data

- Need a normal profile
- Can show variations
  - Top ten web sites
  - Top ten internal users
  - unusual web addresses and ports
  - Which processes/services transfer the most data
- Immune to encryption



# Summary of NBE

- Each method of NBE has its merits and demerits
- No single form of NBE can completely describe an intrusion
- However, evidence “off the wire” can provide critical insights into an intrusion

# Honeynets

- A good way to find popular network attack methods is to use a honeynet
- This provides awareness, information and tools
- Honeynets comprise honeypots and honeywalls
- A honeypot is a network device with weak defences that advertises its contents which are actually of no value
- A honeywall monitors what attackers try to do to access a honeypot

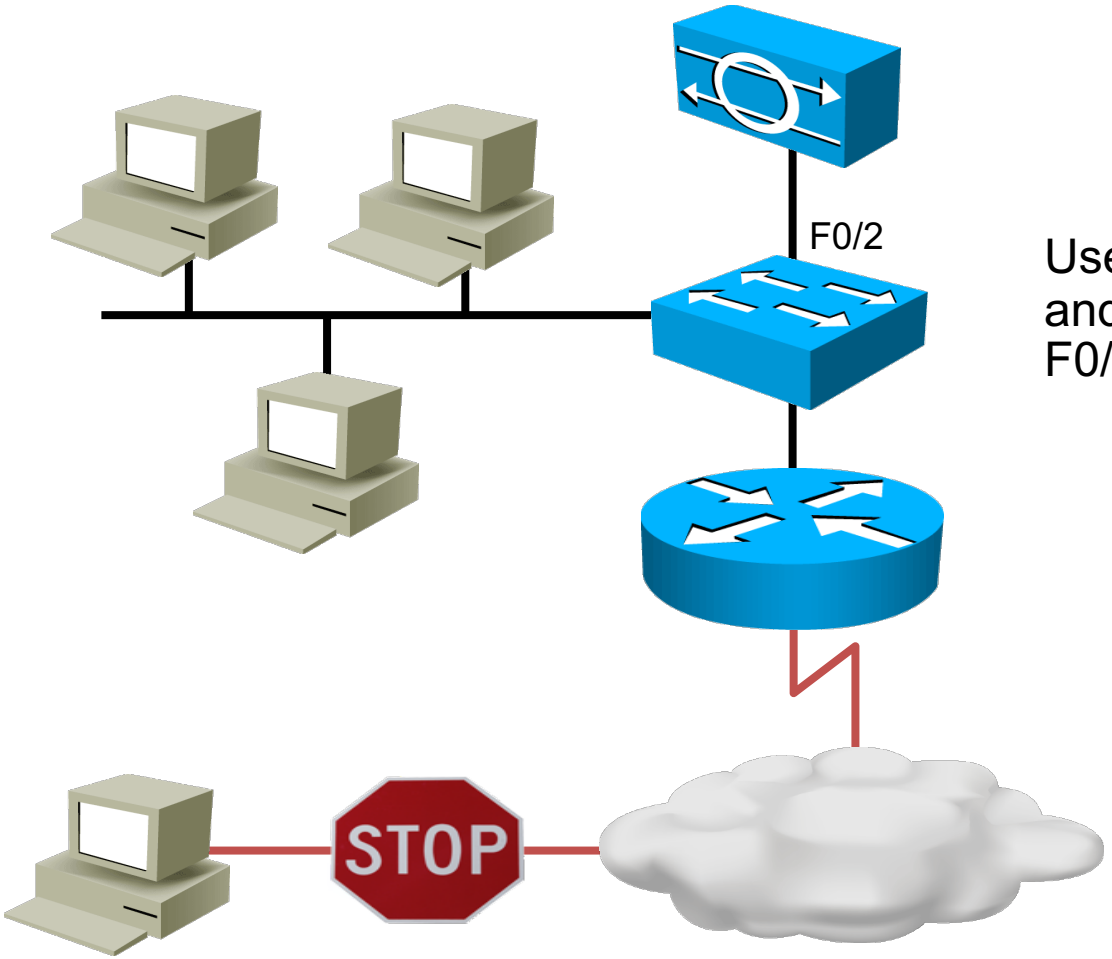
# Honeywall basics

- Why? To answer to the following questions:
- Which protocols does my adversary try to brute-force?
- Which username and password did he use?
- At which speed did he brute-force?
- From where did he proxy from?
- What time of day did he brute-force?

# Accessing the wire

- Two main methods
- Place the pcap device on the wire between the edge router and the firewall
  - either use a hub
  - or two interface cards as a bridge
- Use a switch running span
  - Switch port analyser
  - built into Cisco switches

# Span




Use SPAN to mirror traffic in and out of port F0/1 to port F0/2.

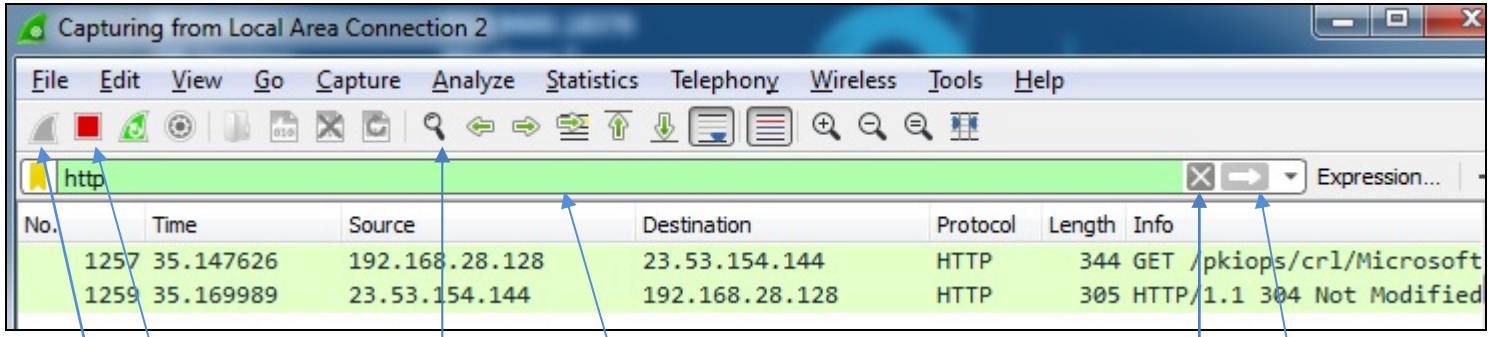
# NBE packet analysers

- The best tools run on Linux FreeBSD
- tcpdump for full content capture
- Winpcap is a Windows version of libpcap
- Windump is the Windows version of tcpdump
- Packets are analysed using Wireshark or Snort
  - online or from a packet dump
- Use tcpview to see session data
- Use Snort to provide alert data in addition to the IPS

# Objectives

- To understand network abuse/attack basics
- To classify methods of collecting network evidence
- To revise the features of Wireshark
- How to use packet captures to baseline a device NBE

# The Wireshark Controls - version 2




Start capture

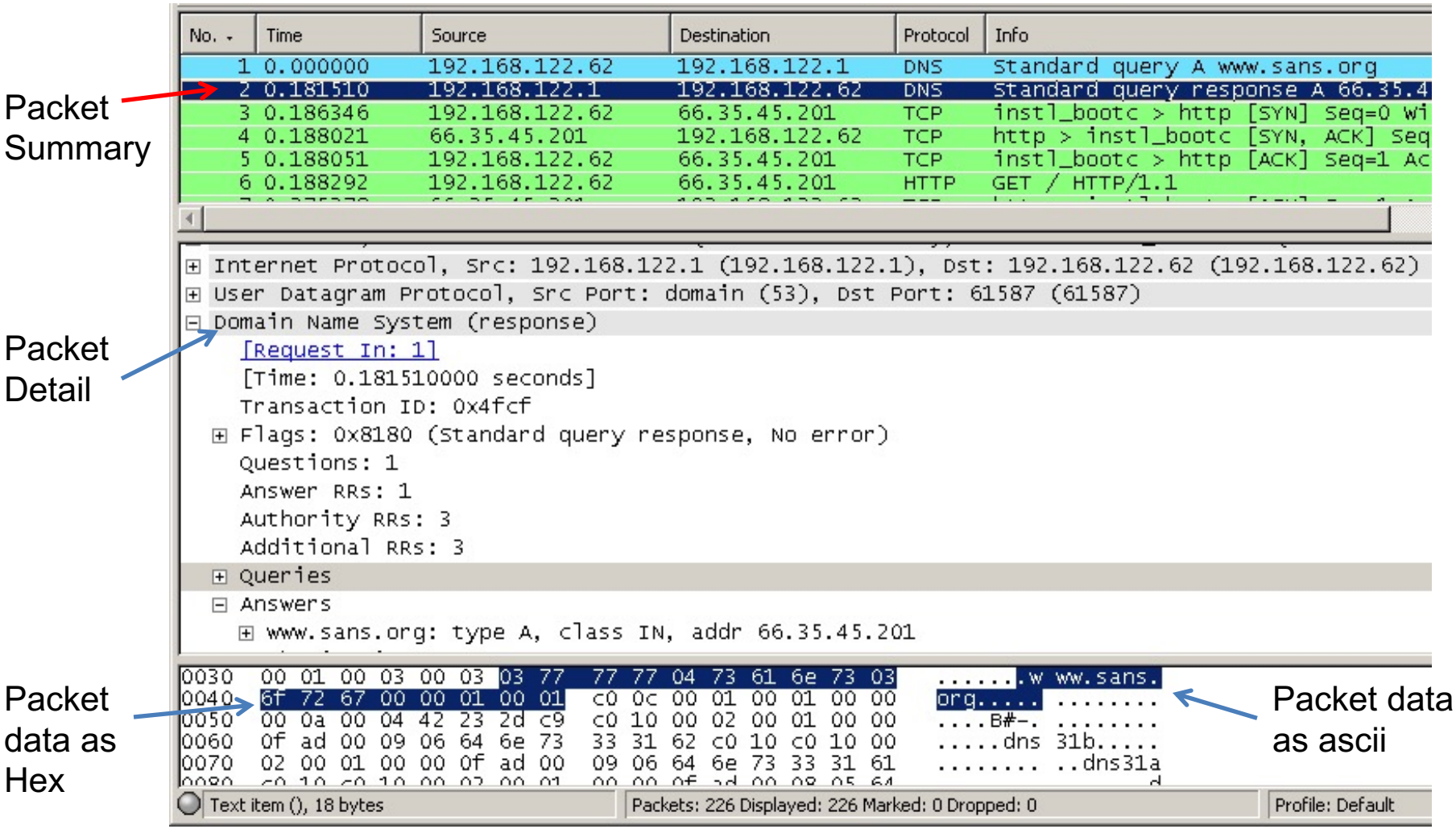
Stop capture

Find a packet

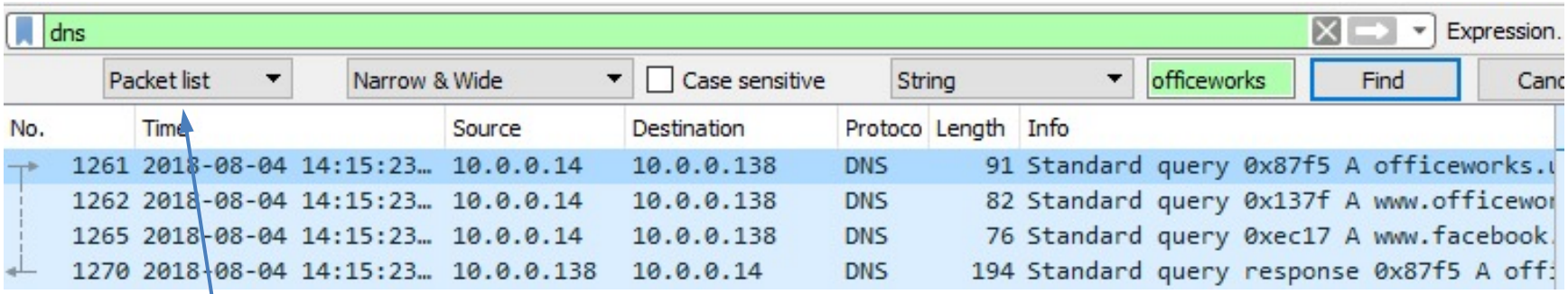
Filter captured packets, click to apply

Clear the filter

# The Wireshark Windows

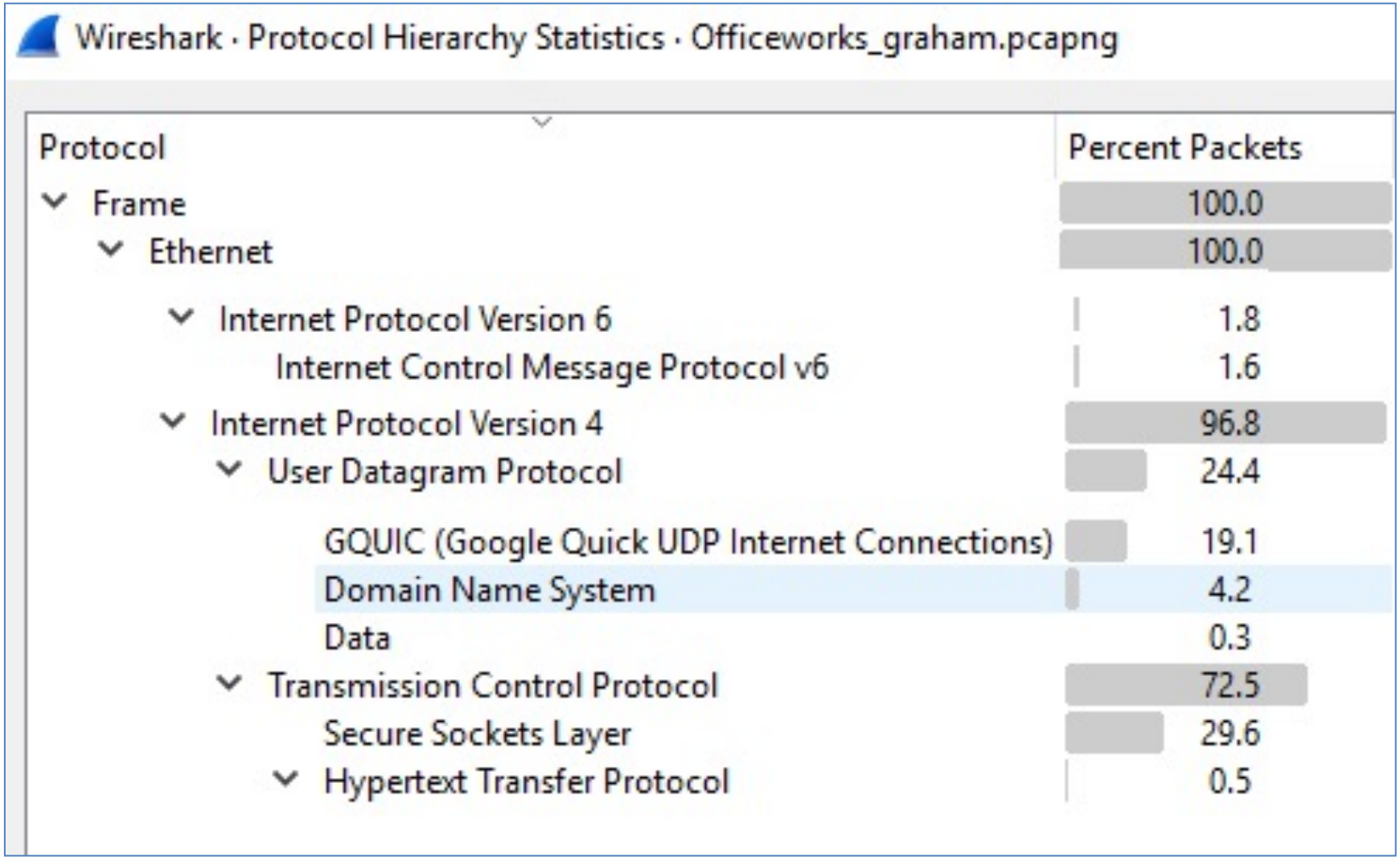


# Wireshark searching v2




- Can search each packet level
- Summary (List)
- Packet Detail
- Data (Bytes)

# Wireshark Statistics



# Wireshark Session

sort by time (seconds)

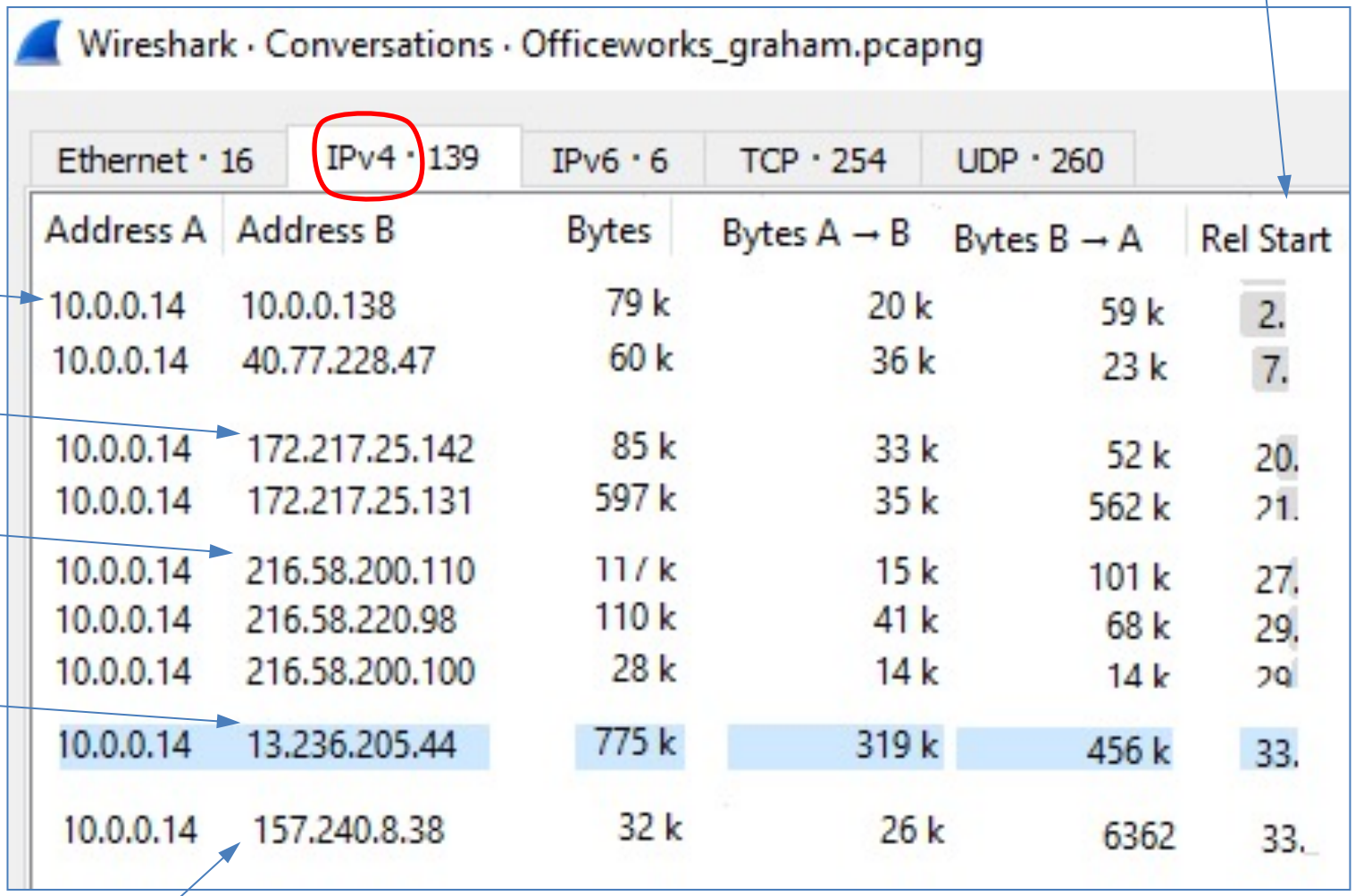
Local Target

YouTube (3rd party)

DoubleClick (3rd party)

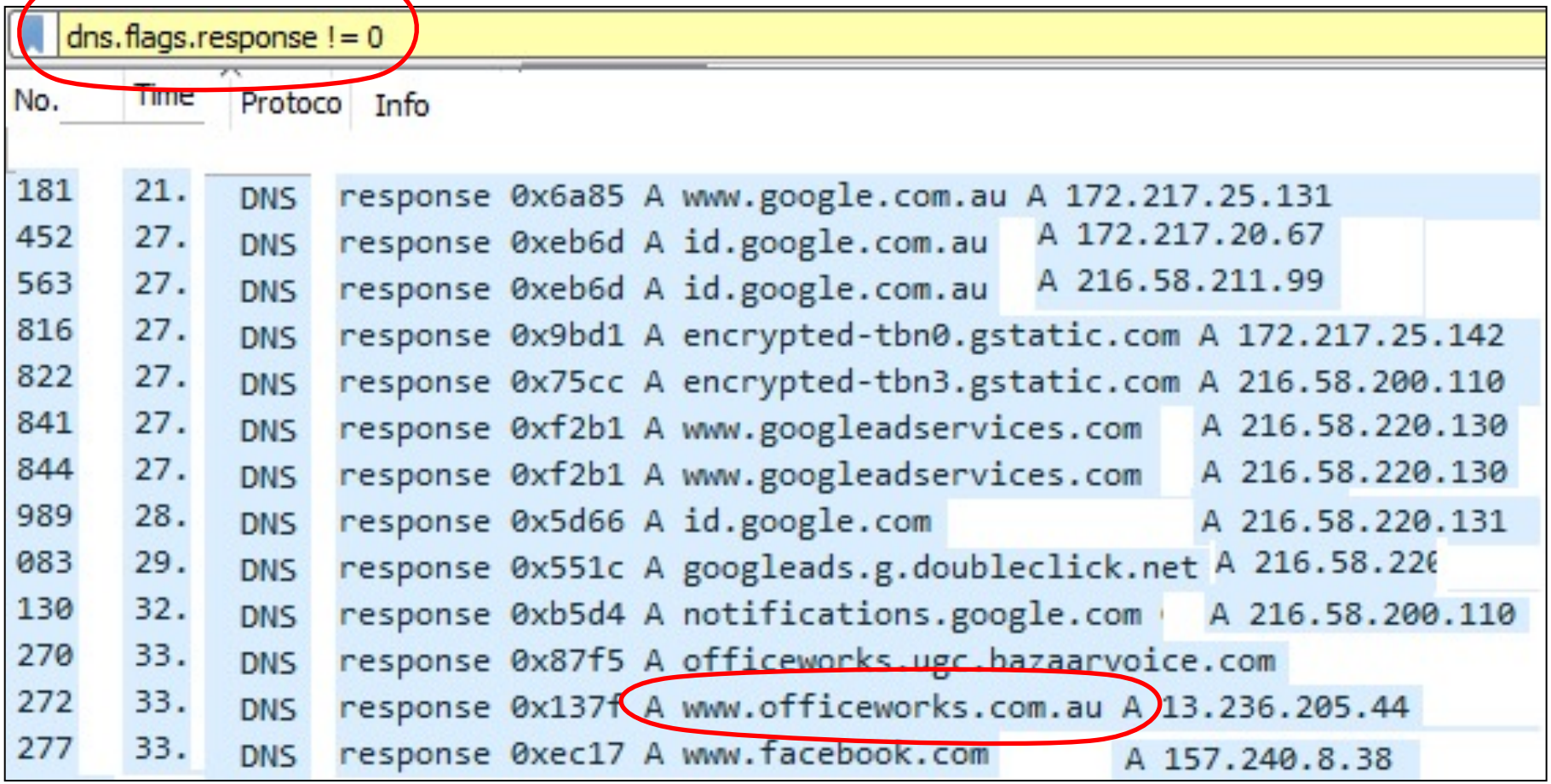
Remote Website on AWS Cloud

Facebook




| Address A | Address B | Bytes | Bytes A → B | Bytes B → A | Rel Start |
|---|---|---|---|---|---|
| 10.0.0.14 | 10.0.0.138 | 79 k | 20 k | 59 k | 2. |
| 10.0.0.14 | 40.77.228.47 | 60 k | 36 k | 23 k | 7. |
| 10.0.0.14 | 172.217.25.142 | 85 k | 33 k | 52 k | 20. |
| 10.0.0.14 | 172.217.25.131 | 597 k | 35 k | 562 k | 21. |
| 10.0.0.14 | 216.58.200.110 | 117 k | 15 k | 101 k | 27. |
| 10.0.0.14 | 216.58.220.98 | 110 k | 41 k | 68 k | 29. |
| 10.0.0.14 | 216.58.200.100 | 28 k | 14 k | 14 k | 29 |
| 10.0.0.14 | 13.236.205.44 | 775 k | 319 k | 456 k | 33. |
| 10.0.0.14 | 157.240.8.38 | 32 k | 26 k | 6362 | 33. |

# Wireshark dns query sessions



# Wireshark filters

- Need to isolate packets of interest amongst a sea of background traffic
- The filters can be simple
  - ssh
- A bit complex
  - ssl.handshake
- Fairly complex
  - not wlan.fc.type_subtype==8
- More filters in readings online

# Objectives

- To understand network abuse/attack basics
- To classify methods of collecting network evidence
- To revise the features of Wireshark
- How to use packet captures to baseline a device NBE

# Data Sources

- Packets can come live from a device
  - from packet capture (pcap) on the network adaptor
- Packets can come from a pcap file
  - from Wireshark
  - from other capture programs
  - tcpdump
  - Dumpcap
  - text2pcap
  - Snort

# Acquiring a web site access

- Identify the web site address
- Start packet capture
- access the website using the browser
  - may involve the web site cache
- Stop capture
- Analyse the results
  - conversations for ip addresses involved
  - statistics to identify protocols
  - reassembly of web pages visited

# Evidence of Accessing a Web site

- The browser/server http handshake
- CSS and JavaScript download
- Page download
  - Text, gifs and jpegs
  - some may come from the local cache
- Plug-ins started
- Cookies downloaded
- External Page Tracking

# Searching a pcap for URLs

- We find URLs in a pcap file using find, grep or wireshark
- For many files or large files these methods do not scale well
- We can use a python script to find URLs
- We search for words that match a keyword dictionary

# More Protocols in Wireshark

- Wireshark provides tools to dig out evidence
- A suspect logging onto a remote site (SSH)
- A Suspect using a VPN (ISAKMP, ESP, AH)
- A suspect accessing a bank web site
  - X.509 Certificates (SSL)
- A suspect using Wireless (802.11)
- A suspect using VOIP (SIP)
- http://www.netresec.com/?page=PcapFiles

# Wireless radio frame capture

- Captures available Wireless Access Points (WAPs)
  - whether they are broadcasting or not
- Windows requires Wireshark in  monitor mode
- a special USB Wireless adaptor
  - Airpcap
- or npcap with usbcap
- Linux can use software on other wireless adaptors
  - Such as aircrack-ng
  - available on the Kali distro
  - Requires a USB wireless card such as TP-Link

# Fin

- Ciao