Pre-Lecture Activities

- There are ***no*** **pre-lecture review questions** for today
- But **please check** the following:
  - The Canvas discussion thread on the **finalized team list**
  - The **group-project brief** uploaded to Canvas

IFS4102: Digital Forensics

Lecture 7: Network & Internet Forensics

Outline

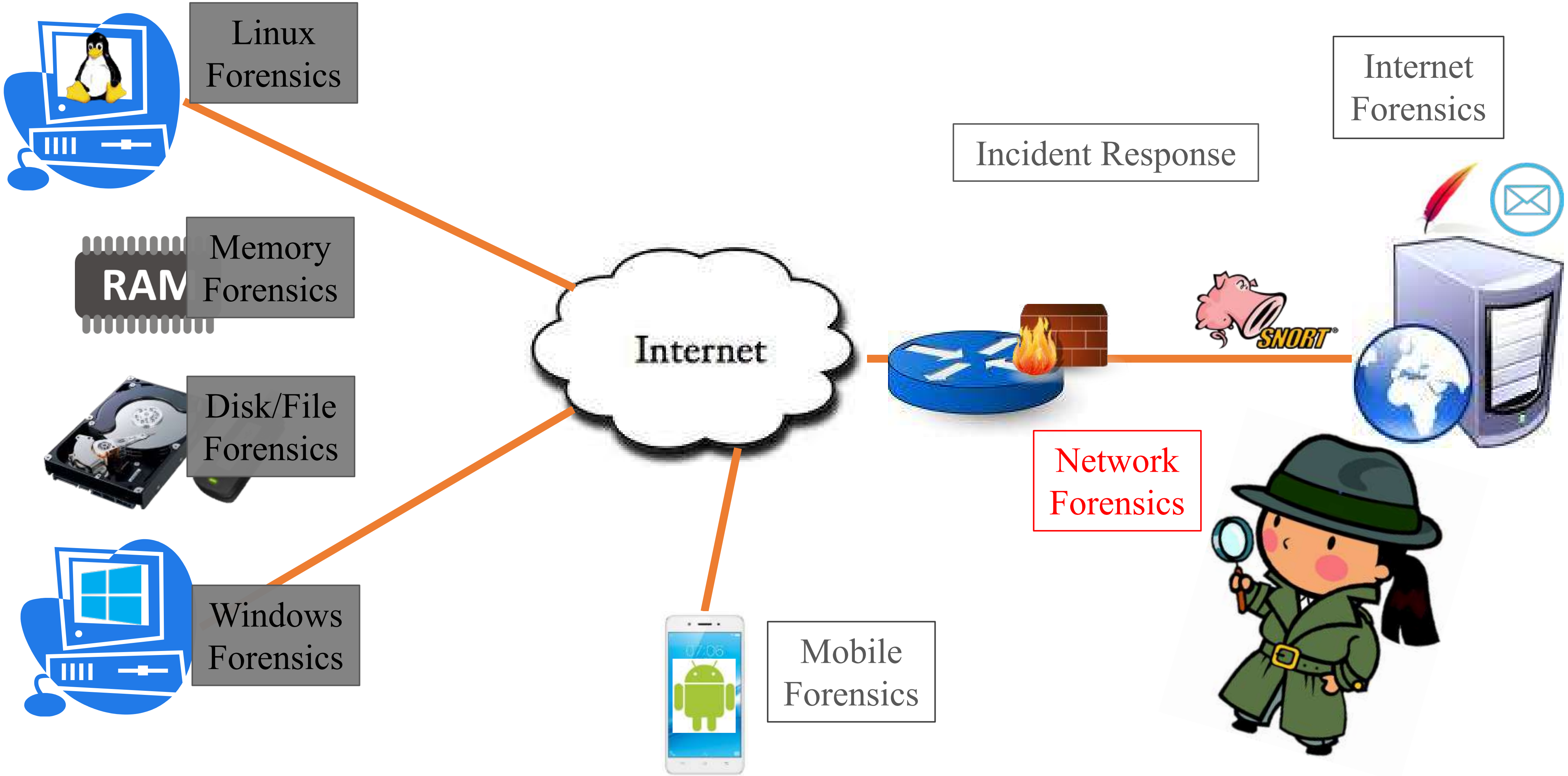
- Network forensics
- Host’s network-setting analysis
- Network traffic analysis
- Network Forensics Analysis Tools: NetworkMiner & Xplico
- Network log analysis

- Internet forensics
- Web artefacts
- Email artefacts
- Lab 7 exercises

- ***Mid-term exam arrangements***
- ***Group-project briefing***

Network Forensics

This Lecture's Focus



Linux Forensics

Memory Forensics

Disk/File Forensics

Windows Forensics

Internet

Mobile Forensics

Incident Response

Internet Forensics

Network Forensics

“Data in Transit” vs “Data at Rest”

- ***Data in transit***:
  - Data **communicated** over networking and/or telco systems
  - From leaving the **sender’s system**, until it becomes accessible to the intended **recipient** of the communication
  - Covered by **network & Internet forensics**
- ***Data at rest***:
  - Data **stored** in non-volatile memory devices
  - Includes "***stored communication***“: a communication that is ***not*** passing over a networking and/or telco system
  - Covered by **disk & file forensics**

Network vs Internet Forensics

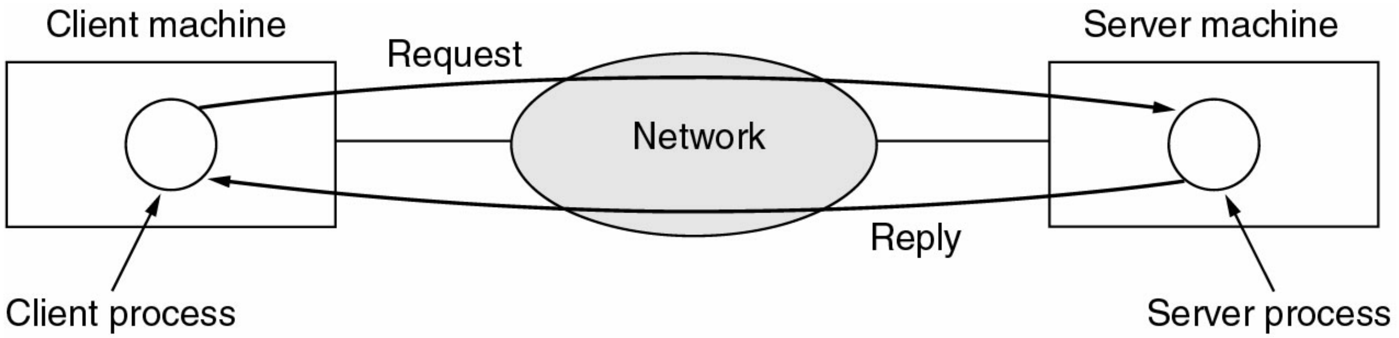
- ***Network forensics*** covers:
  - Network **setting/configuration**
  - Network **traffic analysis**, including ***objects*** contained in the traffic
- ***Internet forensics*** covers:
  - **Email**: transferred email messages, email mailboxes
  - **Web**: HTTP request & response messages, HTTP server's files & log, browser's stored & residual data
  - **DNS**
  - Various other ***networking applications***

Networking Skill for Digital Evidence Examiners

- **Networking knowledge** and skill are so **important** in digital forensics: ***Why?***
  - Almost all systems work in a **networked *environment*** now: over networking and/or telecommunication systems
  - Widely-used **network-based *applications*** with huge user base
- A digital forensics investigator needs to **understand**:
  - How **the networks operate**; and
  - What **potential evidence** is available
- In addition to **content**, we are often also interested in identifying the **source** of activity itself: ***attribution***

Review

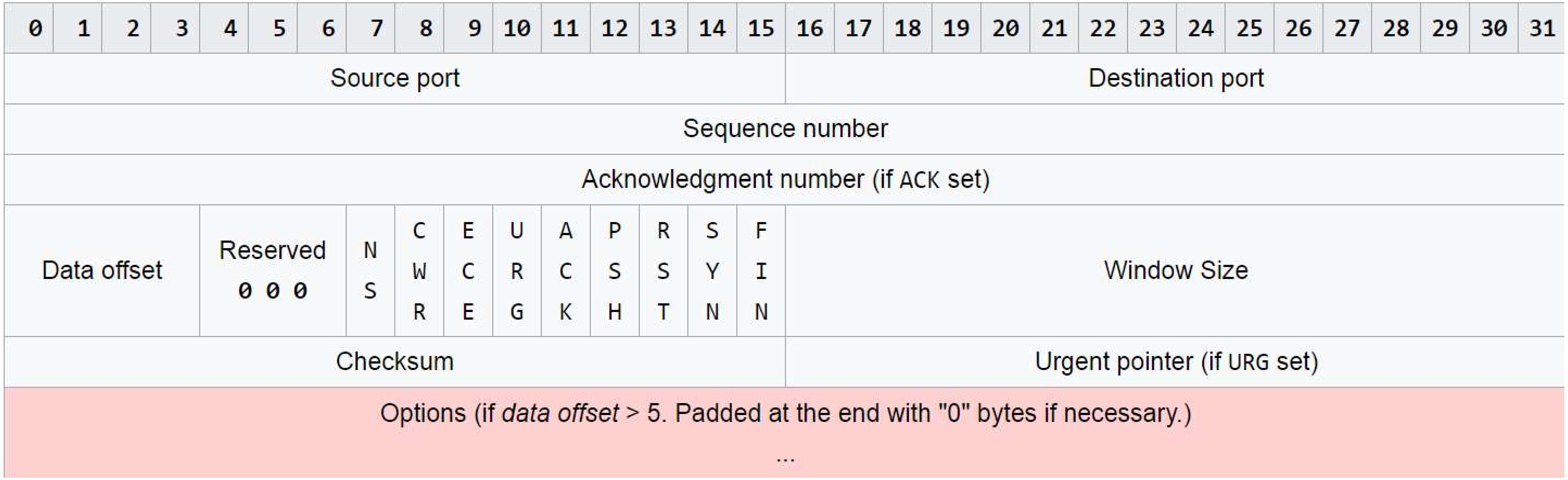
“Client Server” Network-Access Model



Review

TCP

- TCP header format:



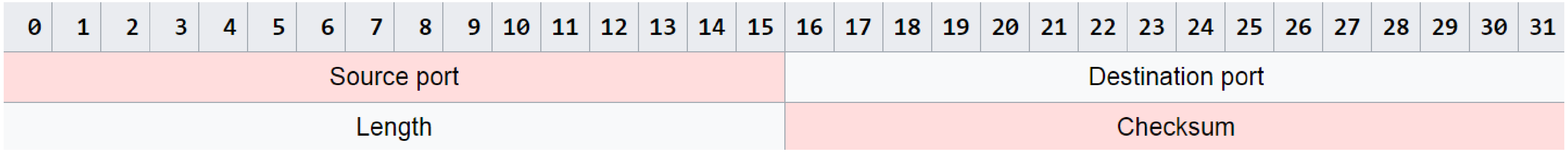
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source port																Destination port															
Sequence number																															
Acknowledgment number (if ACK set)																															
Data offset				Reserved 0 0 0			NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
Checksum																Urgent pointer (if URG set)															
Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

Source: Wikipedia

Review

UDP

- UDP header format:



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source port																Destination port															
Length																Checksum															

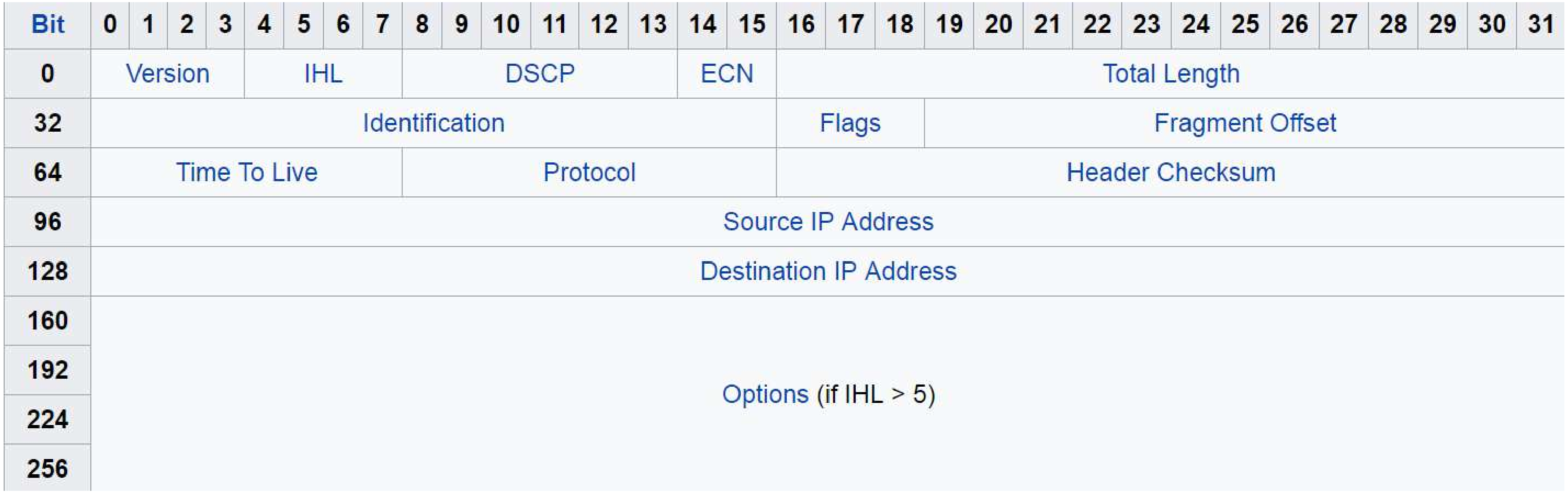
Source: Wikipedia

- Used among others by DNS (port 53), BOOTP/DHCP (port 67 & 68), TFTP (port 69), SNMP (port 161)
- Note: for a list of TCP and UDP **port numbers**, check: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Review

IP

- IP header format:



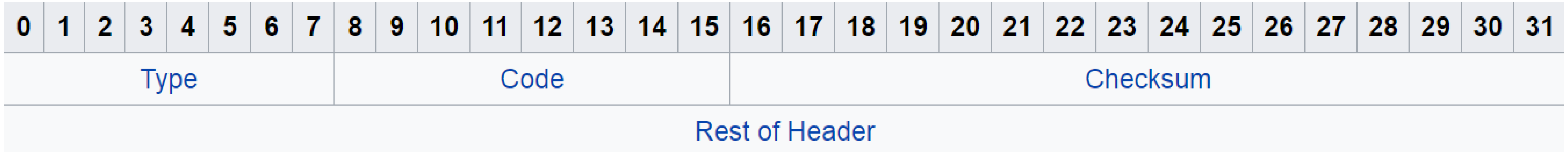
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Version				IHL				DSCP						ECN		Total Length															
32	Identification																Flags			Fragment Offset												
64	Time To Live								Protocol								Header Checksum															
96	Source IP Address																															
128	Destination IP Address																															
160	Options (if IHL > 5)																															
192																																
224																																
256																																

Source: Wikipedia

Review

ICMP

- A supporting protocol for sending error messages & operational information
- Used by **ping** & **traceroute** tools
- ICMP header format:



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type								Code								Checksum															
Rest of Header																															

Source: Wikipedia

- Some control messages (with their **ICMP Types**):
  - Echo Reply (0), Destination Unreachable (3), Redirect Message (5), Echo Request (8), Time Exceeded (11), Parameter Problem: Bad IP header (12)

Network Forensics: Definition & Artefacts

- ***Network forensics***: “the capture, recording & analysis of ***network events*** in order to **discover** the source of security attacks or other problem incidents” (Garfinkel)
- Relevant **network artefacts**:
  - **Host’s** network **configuration**/settings & **logs**
  - Captured **network traffic**: by a packet sniffer (e.g. Wireshark)
  - **Router** and other **networking-device** data:
    NVRAM for configuration files, RAM, logs
  - **Firewall** setting & logs
  - **IDS** setting & logs
  - **SIEM** logs
  - …

Host’s Network-Setting Analysis

Host's Network Settings

- **Live analysis**:
  - Live analysis on an accessible machine
  - **Networking commands** on Windows & Linux: *see the next few slides*
- **Offline analysis**:
  - Analysis of **volatile** memory image:
    - **Volatility** & its relevant networking-related commands (covered earlier)
  - Analysis of **non-volatile** (disk) image:
    - Windows: **registry analysis**
      - Manual analysis: using RegEdit
      - ***Automated analysis***: tools like MiTeC Windows Registry Recovery (WRR) - **See Lab 7**
    - Linux: **network configuration files**

Computer Network Configuration

- **Information needed** to connect a computer to the Internet:
  - IP Address
  - Network mask
  - Gateway
  - DNS server
  - …
- *How to obtain such information?*
  - Automatic setting through DHCP
  - Manual setting

Some Useful Networking Commands (Linux)

- Check & start/stop network interfaces using **`ifconfig`** :
  - List **network interfaces**:
    - **All** interfaces (up and down) whose drivers are loaded:

```
$ ifconfig -a
```

    - All interfaces that are **up**:

```
$ ifconfig
```

    - A **particular** interface (e.g. eth0):

```
$ ifconfig eth0
```

  - **Start & stop** a network interface (e.g. eth0):

```
$ ifconfig eth0 down
$ ifconfig eth0 up
```

Some Useful Networking Commands (Windows)

- Check & start/stop network interfaces using **`ipconfig`** :
  - Usual **network-interface management** commands
  - Additionally for managing **DNS cache**:

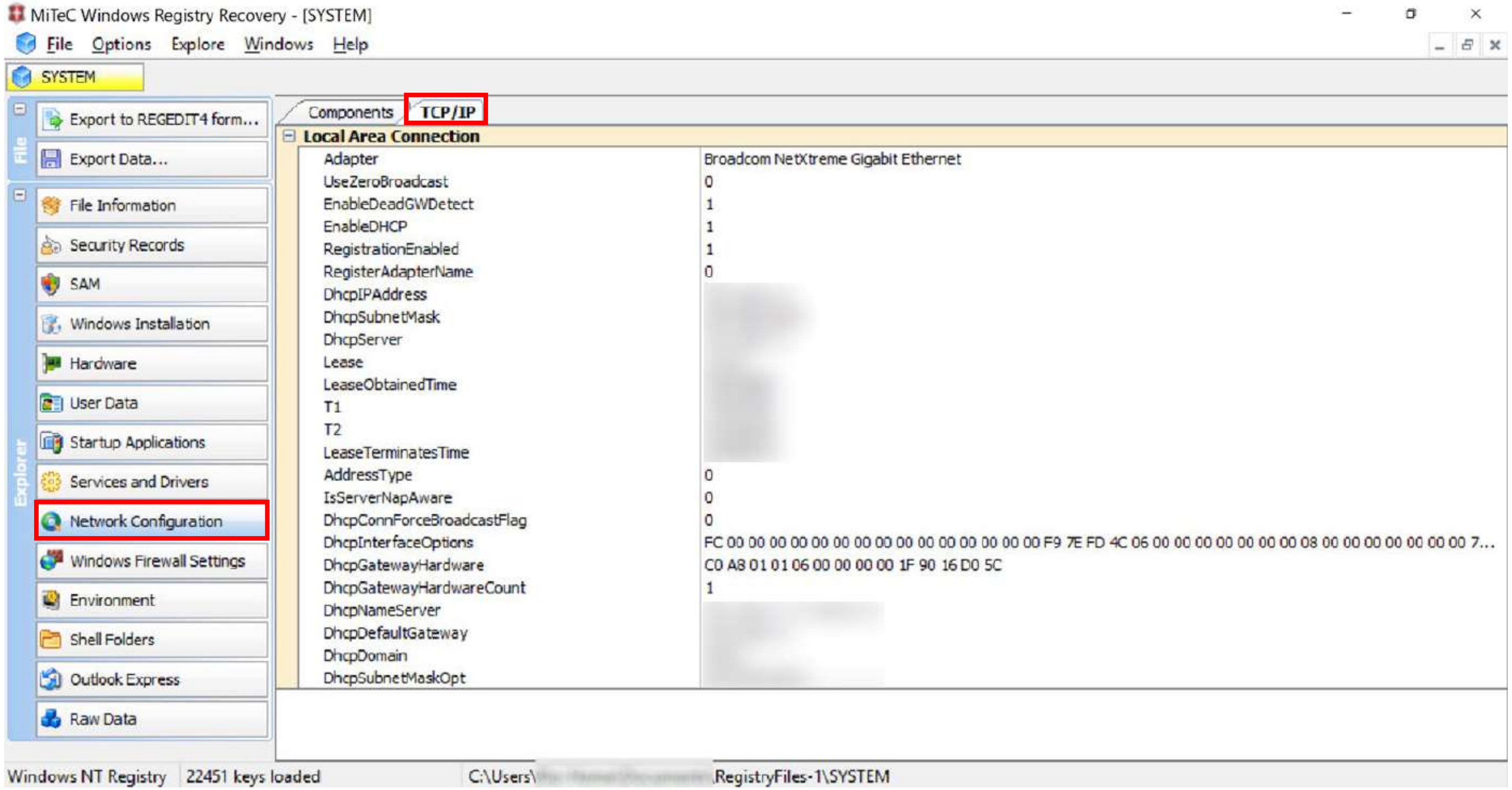
```
> ipconfig /displaydns

> ipconfig /flushdns

> ipconfig /registerdns
```

  - As well as checking **DNS server**:

```
> netsh interface ipv4 show dnsservers
```

Windows Registry Recovery (WRR)

- **TCP/IP setting**:



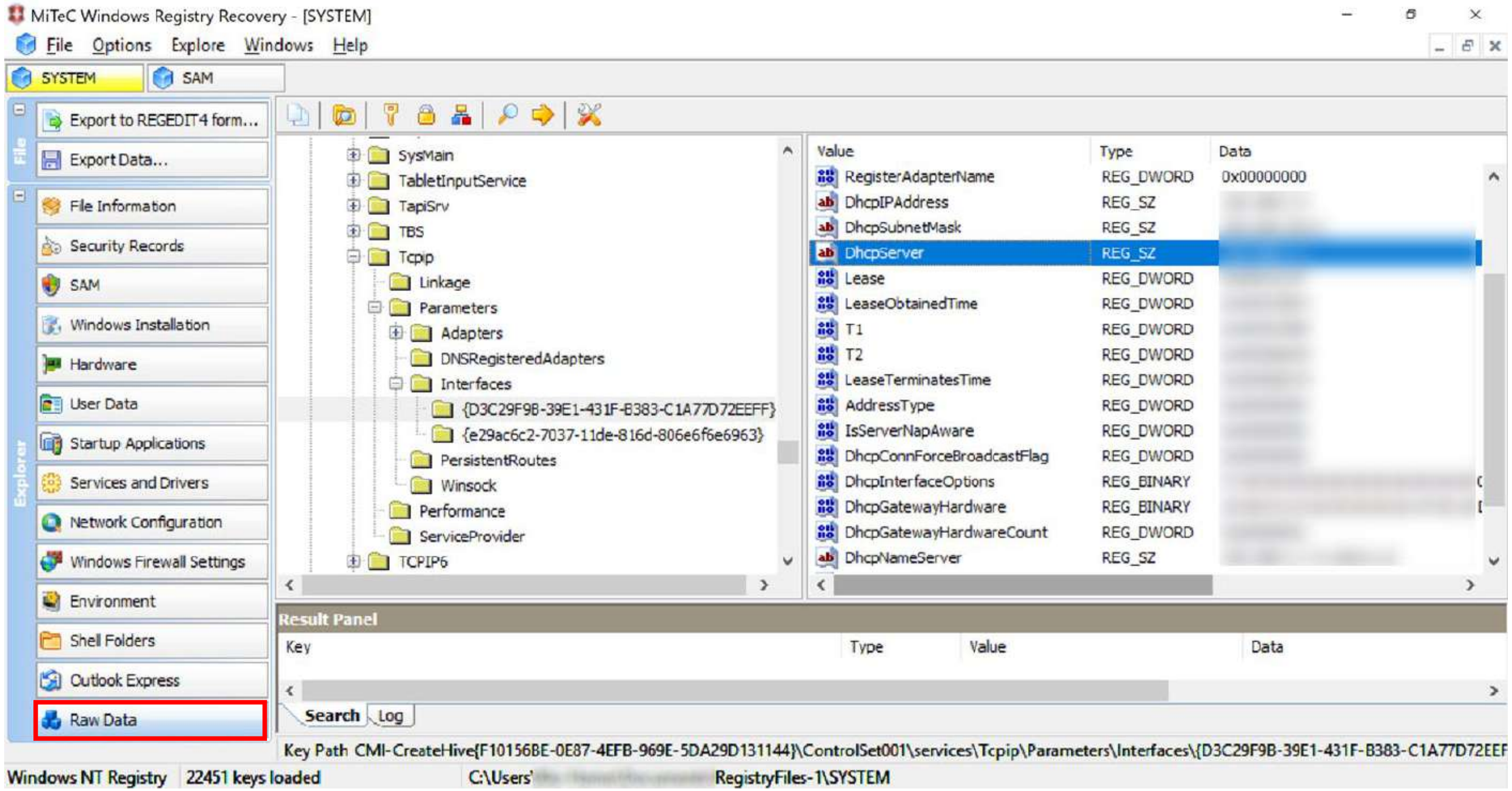
Local Area Connection

Adapter	Broadcom NetXtreme Gigabit Ethernet
UseZeroBroadcast	0
EnableDeadGWDetect	1
EnableDHCP	1
RegistrationEnabled	1
RegisterAdapterName	0
DhcpIPAddress	[redacted]
DhcpSubnetMask	[redacted]
DhcpServer	[redacted]
Lease	[redacted]
LeaseObtainedTime	[redacted]
T1	[redacted]
T2	[redacted]
LeaseTerminatesTime	[redacted]
AddressType	0
IsServerNapAware	0
DhcpConnForceBroadcastFlag	0
DhcpInterfaceOptions	FC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F9 7E FD 4C 06 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 7...
DhcpGatewayHardware	C0 A8 01 01 06 00 00 00 00 1F 90 16 D0 5C
DhcpGatewayHardwareCount	1
DhcpNameServer	[redacted]
DhcpDefaultGateway	[redacted]
DhcpDomain	[redacted]
DhcpSubnetMaskOpt	[redacted]

Windows NT Registry | 22451 keys loaded | C:\Users\[redacted]RegistryFiles-1\SYSTEM

Windows Registry Recovery (WRR)

- **Manual/raw** registry-key access:



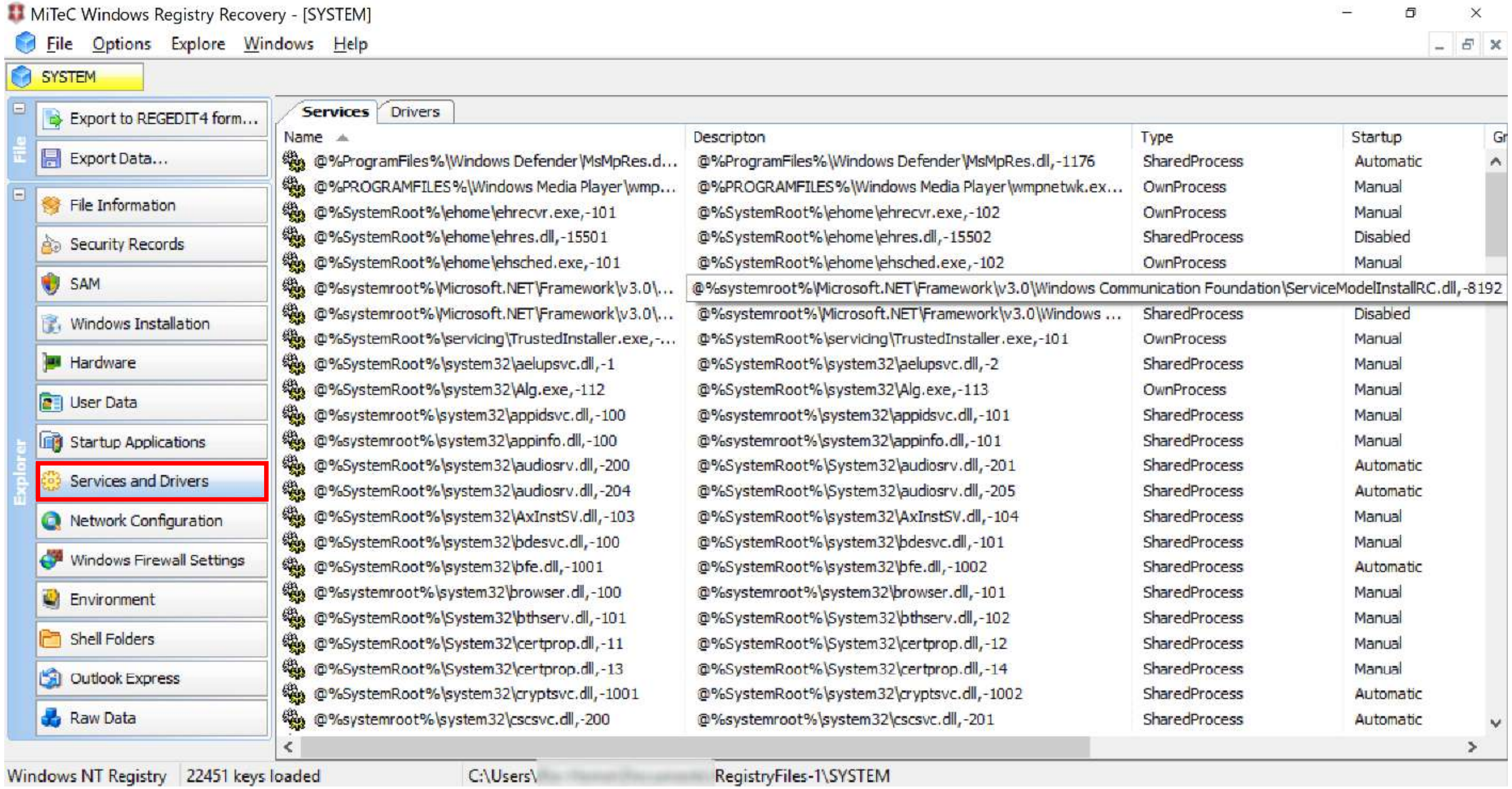
Value	Type	Data
RegisterAdapterName	REG_DWORD	0x00000000
DhcpIPAddress	REG_SZ	[redacted]
DhcpSubnetMask	REG_SZ	[redacted]
DhcpServer	REG_SZ	[redacted]
Lease	REG_DWORD	[redacted]
LeaseObtainedTime	REG_DWORD	[redacted]
T1	REG_DWORD	[redacted]
T2	REG_DWORD	[redacted]
LeaseTerminatesTime	REG_DWORD	[redacted]
AddressType	REG_DWORD	[redacted]
IsServerNapAware	REG_DWORD	[redacted]
DhcpConnForceBroadcastFlag	REG_DWORD	[redacted]
DhcpInterfaceOptions	REG_BINARY	[redacted]
DhcpGatewayHardware	REG_BINARY	[redacted]
DhcpGatewayHardwareCount	REG_DWORD	[redacted]
DhcpNameServer	REG_SZ	[redacted]

Key Path CMI-CreateHive{F10156BE-0E87-4EFB-969E-5DA29D131144}\ControlSet001\services\Tcpip\Parameters\Interfaces\{D3C29F9B-39E1-431F-B383-C1A77D72EEF

Windows NT Registry | 22451 keys loaded | C:\Users\[redacted]RegistryFiles-1\SYSTEM

Windows Registry Recovery (WRR)

- **Services and drivers:**

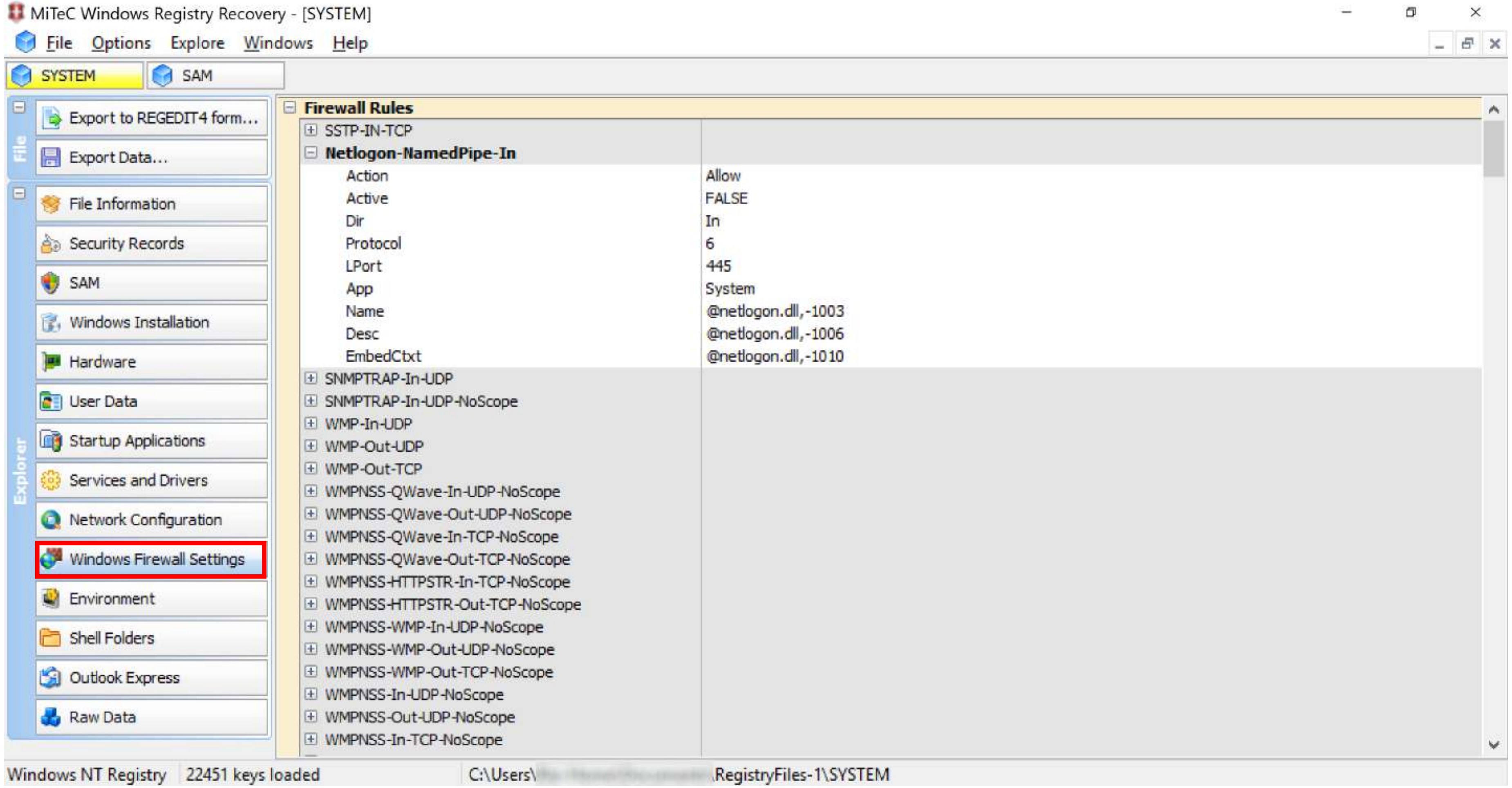


Name	Descripton	Type	Startup	Gr
@%ProgramFiles%\Windows Defender\MsMpRes.d...	@%ProgramFiles%\Windows Defender\MsMpRes.dll,-1176	SharedProcess	Automatic	
@%PROGRAMFILES%\Windows Media Player\wmp...	@%PROGRAMFILES%\Windows Media Player\wmpnetwk.ex...	OwnProcess	Manual	
@%SystemRoot%\ehome\ehrecvr.exe,-101	@%SystemRoot%\ehome\ehrecvr.exe,-102	OwnProcess	Manual	
@%SystemRoot%\ehome\ehres.dll,-15501	@%SystemRoot%\ehome\ehres.dll,-15502	SharedProcess	Disabled	
@%SystemRoot%\ehome\ehsched.exe,-101	@%SystemRoot%\ehome\ehsched.exe,-102	OwnProcess	Manual	
@%systemroot%\Microsoft.NET\Framework\v3.0\...	@%systemroot%\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\ServiceModelInstallRC.dll,-8192			
@%systemroot%\Microsoft.NET\Framework\v3.0\...	@%systemroot%\Microsoft.NET\Framework\v3.0\Windows ...	SharedProcess	Disabled	
@%SystemRoot%\servicing\TrustedInstaller.exe,-...	@%SystemRoot%\servicing\TrustedInstaller.exe,-101	OwnProcess	Manual	
@%SystemRoot%\system32\aelupsvc.dll,-1	@%SystemRoot%\system32\aelupsvc.dll,-2	SharedProcess	Manual	
@%SystemRoot%\system32\Alg.exe,-112	@%SystemRoot%\system32\Alg.exe,-113	OwnProcess	Manual	
@%systemroot%\system32\appidsvc.dll,-100	@%systemroot%\system32\appidsvc.dll,-101	SharedProcess	Manual	
@%systemroot%\system32\appinfo.dll,-100	@%systemroot%\system32\appinfo.dll,-101	SharedProcess	Manual	
@%SystemRoot%\system32\audiosrv.dll,-200	@%SystemRoot%\System32\audiosrv.dll,-201	SharedProcess	Automatic	
@%SystemRoot%\system32\audiosrv.dll,-204	@%SystemRoot%\System32\audiosrv.dll,-205	SharedProcess	Automatic	
@%SystemRoot%\system32\AxInstSV.dll,-103	@%SystemRoot%\system32\AxInstSV.dll,-104	SharedProcess	Manual	
@%SystemRoot%\system32\bdesvc.dll,-100	@%SystemRoot%\system32\bdesvc.dll,-101	SharedProcess	Manual	
@%SystemRoot%\system32\bfe.dll,-1001	@%SystemRoot%\system32\bfe.dll,-1002	SharedProcess	Automatic	
@%systemroot%\system32\browser.dll,-100	@%systemroot%\system32\browser.dll,-101	SharedProcess	Manual	
@%SystemRoot%\System32\bthserv.dll,-101	@%SystemRoot%\System32\bthserv.dll,-102	SharedProcess	Manual	
@%SystemRoot%\System32\certprop.dll,-11	@%SystemRoot%\System32\certprop.dll,-12	SharedProcess	Manual	
@%SystemRoot%\System32\certprop.dll,-13	@%SystemRoot%\System32\certprop.dll,-14	SharedProcess	Manual	
@%SystemRoot%\system32\cryptsvc.dll,-1001	@%SystemRoot%\system32\cryptsvc.dll,-1002	SharedProcess	Automatic	
@%systemroot%\system32\cscsvc.dll,-200	@%systemroot%\system32\cscsvc.dll,-201	SharedProcess	Automatic	

Windows NT Registry | 22451 keys loaded | C:\Users\[redacted]RegistryFiles-1\SYSTEM

Windows Registry Recovery (WRR)

- Windows **firewall settings**:



Firewall Rules

SSTP-IN-TCP

Netlogon-NamedPipe-In

Action	Allow
Active	FALSE
Dir	In
Protocol	6
LPort	445
App	System
Name	@netlogon.dll,-1003
Desc	@netlogon.dll,-1006
EmbedCtxt	@netlogon.dll,-1010

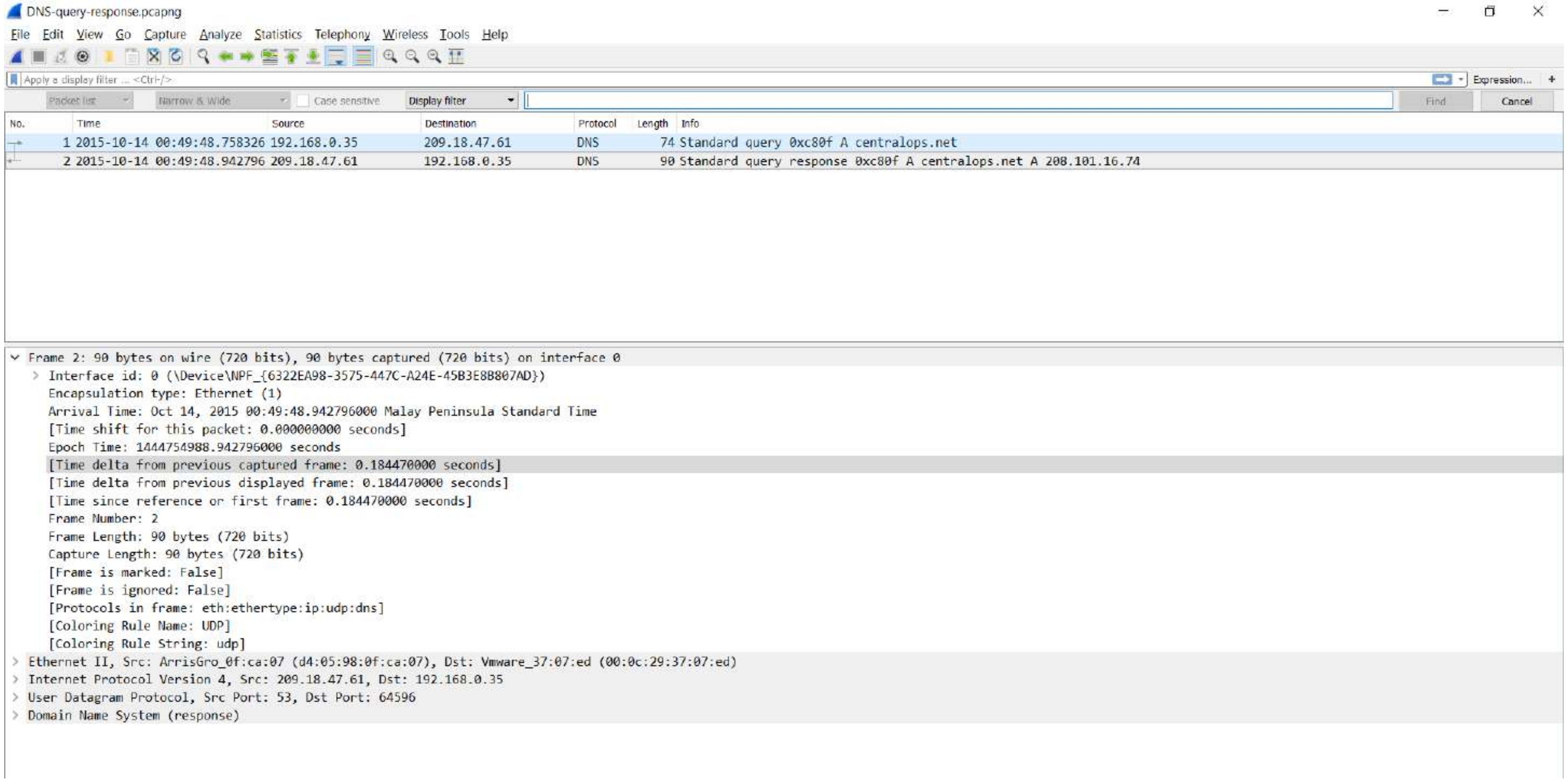
SNMPTRAP-In-UDP
SNMPTRAP-In-UDP-NoScope
WMP-In-UDP
WMP-Out-UDP
WMP-Out-TCP
WMPNSS-QWave-In-UDP-NoScope
WMPNSS-QWave-Out-UDP-NoScope
WMPNSS-QWave-In-TCP-NoScope
WMPNSS-QWave-Out-TCP-NoScope
WMPNSS-HTTPSTR-In-TCP-NoScope
WMPNSS-HTTPSTR-Out-TCP-NoScope
WMPNSS-WMP-In-UDP-NoScope
WMPNSS-WMP-Out-UDP-NoScope
WMPNSS-WMP-Out-TCP-NoScope
WMPNSS-In-UDP-NoScope
WMPNSS-Out-UDP-NoScope
WMPNSS-In-TCP-NoScope

Windows NT Registry | 22451 keys loaded | C:\Users\[redacted]RegistryFiles-1\SYSTEM

Network Traffic Analysis

Network Traffic Analysis

- **Wireshark**: to capture traffic & analyze offline pcap/pcapng files



DNS-query-response.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

```
No.   Time                        Source          Destination     Protocol  Length  Info
    1 2015-10-14 00:49:48.758326 192.168.0.35    209.18.47.61    DNS           74 Standard query 0xc80f A centralops.net
    2 2015-10-14 00:49:48.942796 209.18.47.61    192.168.0.35    DNS           90 Standard query response 0xc80f A centralops.net A 208.101.16.74
```

```
v Frame 2: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
   > Interface id: 0 (\Device\NPF_{6322EA98-3575-447C-A24E-45B3E8B807AD})
     Encapsulation type: Ethernet (1)
     Arrival Time: Oct 14, 2015 00:49:48.942796000 Malay Peninsula Standard Time
     [Time shift for this packet: 0.000000000 seconds]
     Epoch Time: 1444754988.942796000 seconds
     [Time delta from previous captured frame: 0.184470000 seconds]
     [Time delta from previous displayed frame: 0.184470000 seconds]
     [Time since reference or first frame: 0.184470000 seconds]
     Frame Number: 2
     Frame Length: 90 bytes (720 bits)
     Capture Length: 90 bytes (720 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: eth:ethertype:ip:udp:dns]
     [Coloring Rule Name: UDP]
     [Coloring Rule String: udp]
> Ethernet II, Src: ArrisGro_0f:ca:07 (d4:05:98:0f:ca:07), Dst: Vmware_37:07:ed (00:0c:29:37:07:ed)
> Internet Protocol Version 4, Src: 209.18.47.61, Dst: 192.168.0.35
> User Datagram Protocol, Src Port: 53, Dst Port: 64596
> Domain Name System (response)
```

Wireshark: About (Recap)

- Very popular tool:
  No 1 at http://sectools.org/ Top 125 Network Security Tools
- A **network packet/protocol analyzer**
- Used by both **network admins** & **hackers** (white-hat/black-hat)
- For network diagnostic & security purposes

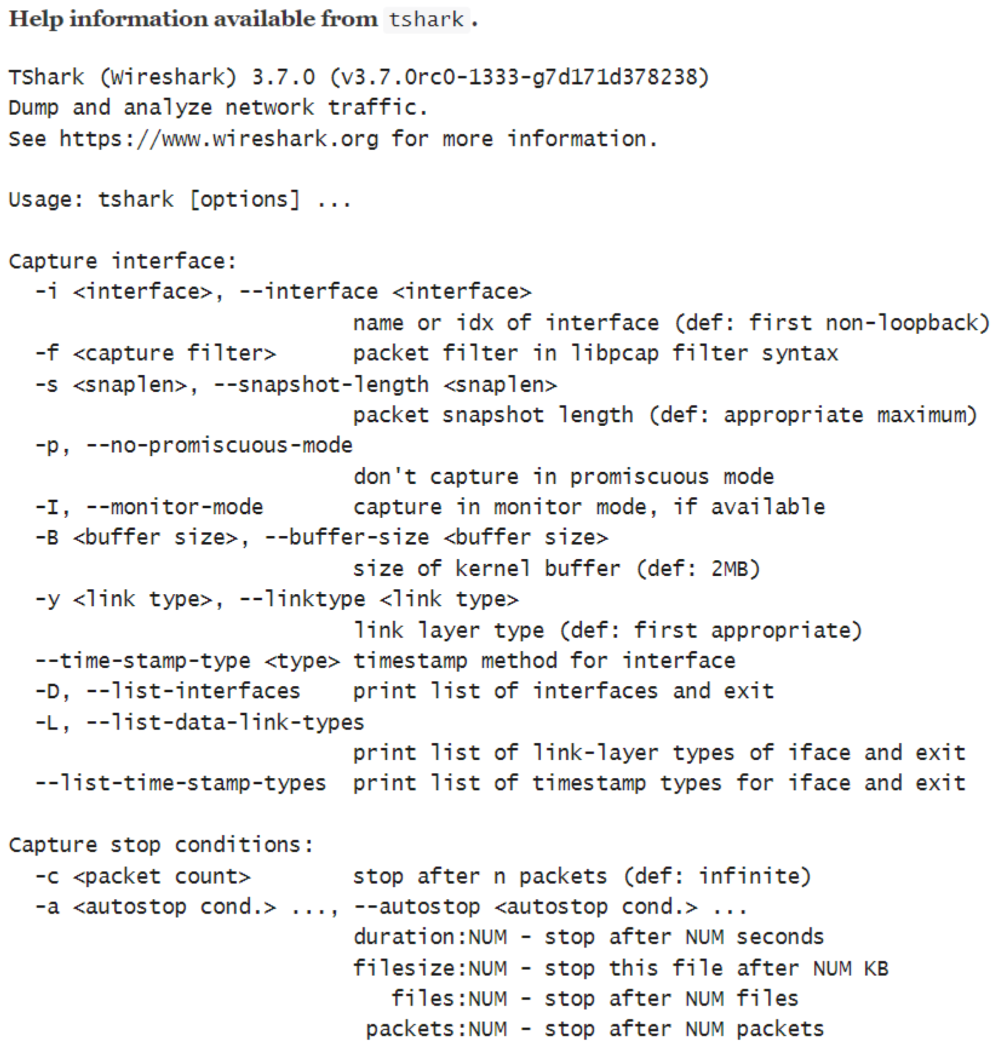
- Many resources available: tutorials, sample captured files, …
- A good **sample demo video** on Wireshak packet filtering
  (for your refresher):
  https://www.youtube.com/watch?v=rlDIlgzyo1Y

Review

Wireshark: Background

- **History**:
  - July 1998: ***Ethereal*** version 0.2.0
  - 2006: the project moved house and re-emerged under a new name *Wireshark*
  - 2008: Wireshark version 1.0
  - 2015: Wireshark 2.0
  - 2018: Version 2.9.0
- Wireshark uses **pcap** to capture packets: **libpcap** (UNIX/Linux) and **WinPcap** (Windows) libraries
- Other alternative tools: tcpdump/Tcptrace, snoop, **TShark (terminal-based Wireshark)**: see also https://www.wireshark.org/docs/wsug_html_chunked/AppTools.html

TShark: Terminal-based Wireshark



Help information available from `tshark`**.**

```
TShark (Wireshark) 3.7.0 (v3.7.0rc0-1333-g7d171d378238)
Dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: tshark [options] ...

Capture interface:
  -i <interface>, --interface <interface>
                           name or idx of interface (def: first non-loopback)
  -f <capture filter>      packet filter in libpcap filter syntax
  -s <snaplen>, --snapshot-length <snaplen>
                           packet snapshot length (def: appropriate maximum)
  -p, --no-promiscuous-mode
                           don't capture in promiscuous mode
  -I, --monitor-mode       capture in monitor mode, if available
  -B <buffer size>, --buffer-size <buffer size>
                           size of kernel buffer (def: 2MB)
  -y <link type>, --linktype <link type>
                           link layer type (def: first appropriate)
  --time-stamp-type <type> timestamp method for interface
  -D, --list-interfaces    print list of interfaces and exit
  -L, --list-data-link-types
                           print list of link-layer types of iface and exit
  --list-time-stamp-types  print list of timestamp types for iface and exit

Capture stop conditions:
  -c <packet count>        stop after n packets (def: infinite)
  -a <autostop cond.> ..., --autostop <autostop cond.> ...
                           duration:NUM - stop after NUM seconds
                           filesize:NUM - stop this file after NUM KB
                              files:NUM - stop after NUM files
                            packets:NUM - stop after NUM packets
```

...

From: https://www.wireshark.org/docs/wsug_html_chunked/AppToolstshark.html

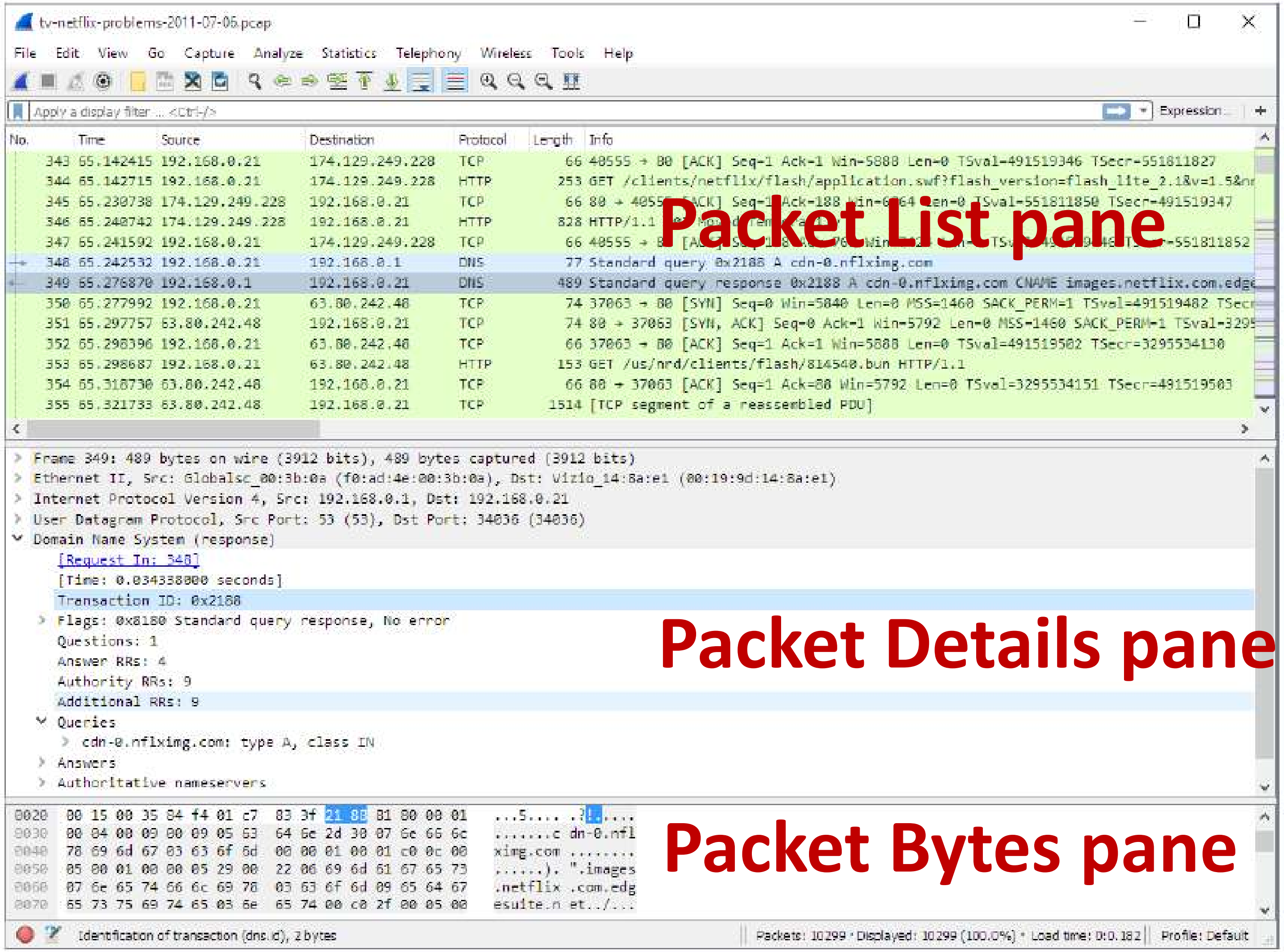
Wireshark Features

- Some good ***features***:
  - **Import** files from other capture programs
  - Nice **GUI**
  - Various protocol **dissectors**
  - **Filter** packets on many criteria
  - **Search** for packets on many criteria.
  - **Colorize** packet display based on filters

- What Wireshark *is **not***?
  - Wireshark is *not* an IDS
  - Wireshark will *not* manipulate things on the network, it will only "*measure*" things from it

Review

Wireshark User Interface


tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time      Source          Destination     Protocol Length Info
 343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
 344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
 345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
 346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
 347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 8[illegible]-551811852
 348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
 349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
 350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
 351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
 352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=329534130
 353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
 354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=329534151 TSecr=491519503
 355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

Packet List pane

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

Packet Details pane

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

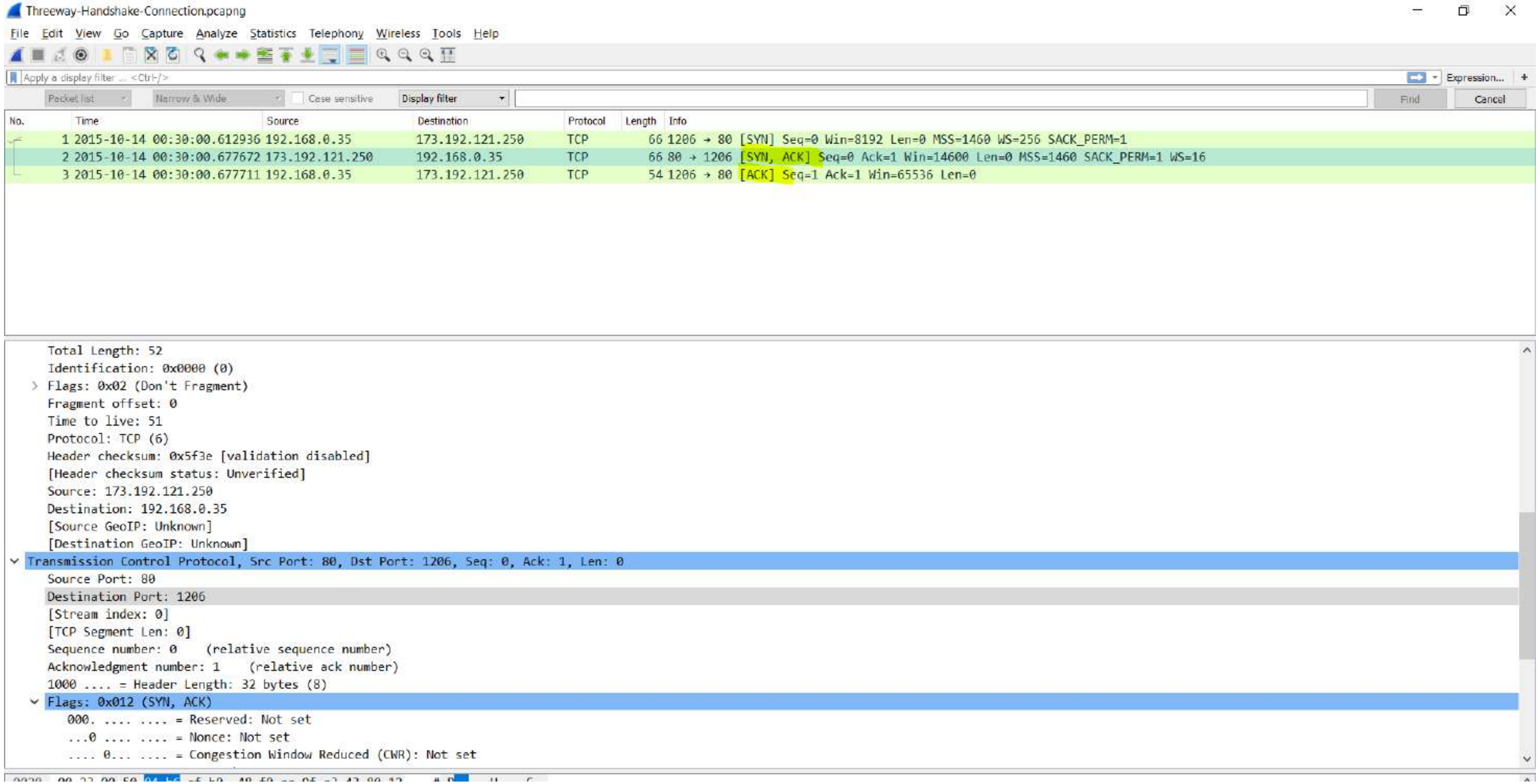
Packet Bytes pane

Identification of transaction (dns.id), 2 bytes
Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182
Profile: Default

Review

Wireshark

- Packet **content** and **flags** analyses:



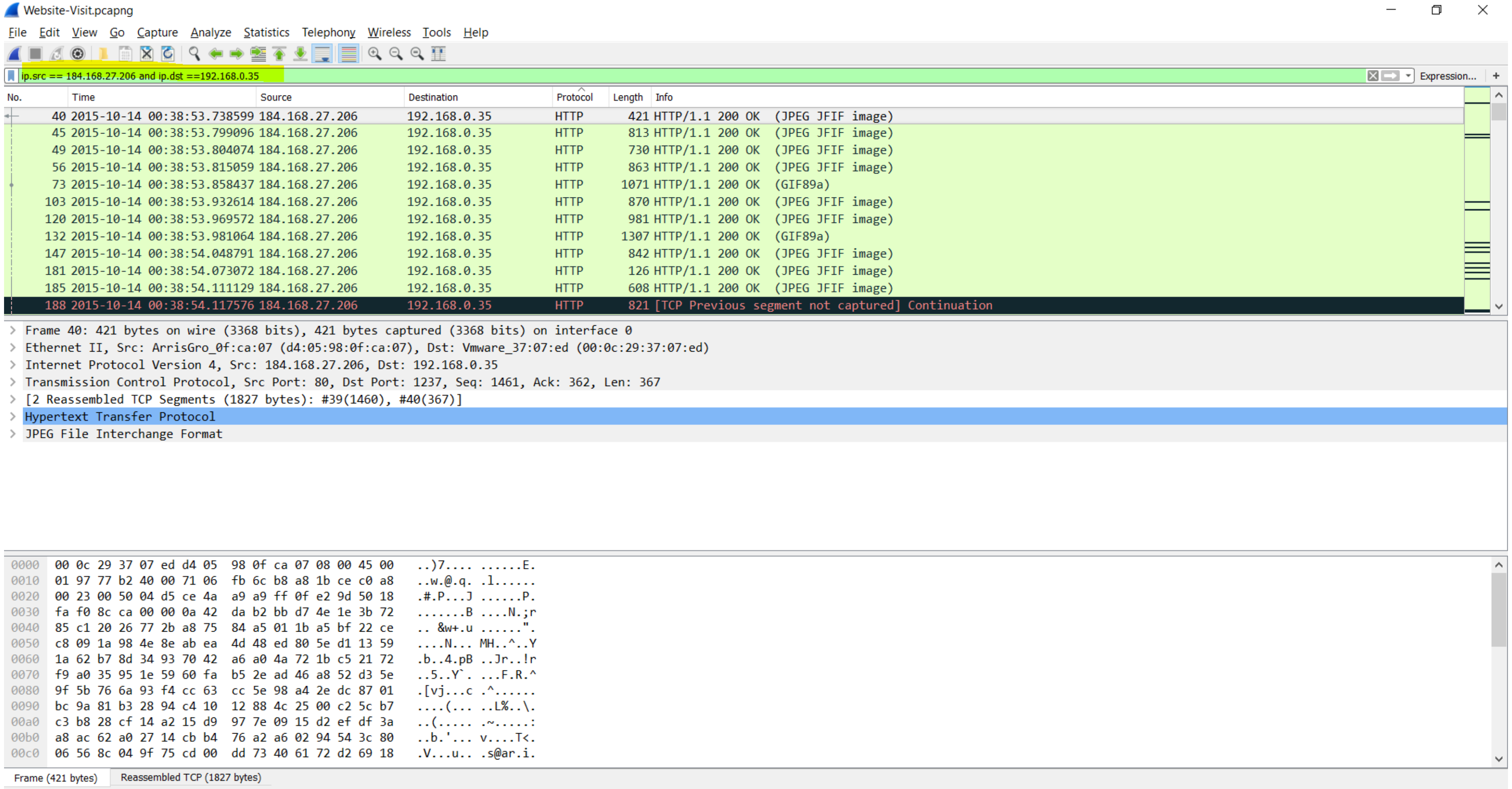
```
No.  Time                        Source           Destination      Protocol  Length Info
   1 2015-10-14 00:30:00.612936 192.168.0.35     173.192.121.250  TCP          66 1206 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   2 2015-10-14 00:30:00.677672 173.192.121.250  192.168.0.35     TCP          66 80 → 1206 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
   3 2015-10-14 00:30:00.677711 192.168.0.35     173.192.121.250  TCP          54 1206 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

```
    Total Length: 52
    Identification: 0x0000 (0)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 51
    Protocol: TCP (6)
    Header checksum: 0x5f3e [validation disabled]
    [Header checksum status: Unverified]
    Source: 173.192.121.250
    Destination: 192.168.0.35
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v Transmission Control Protocol, Src Port: 80, Dst Port: 1206, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 1206
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
```

Review

Wireshark

- Wireshark **display filtering**:


Website-Visit.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

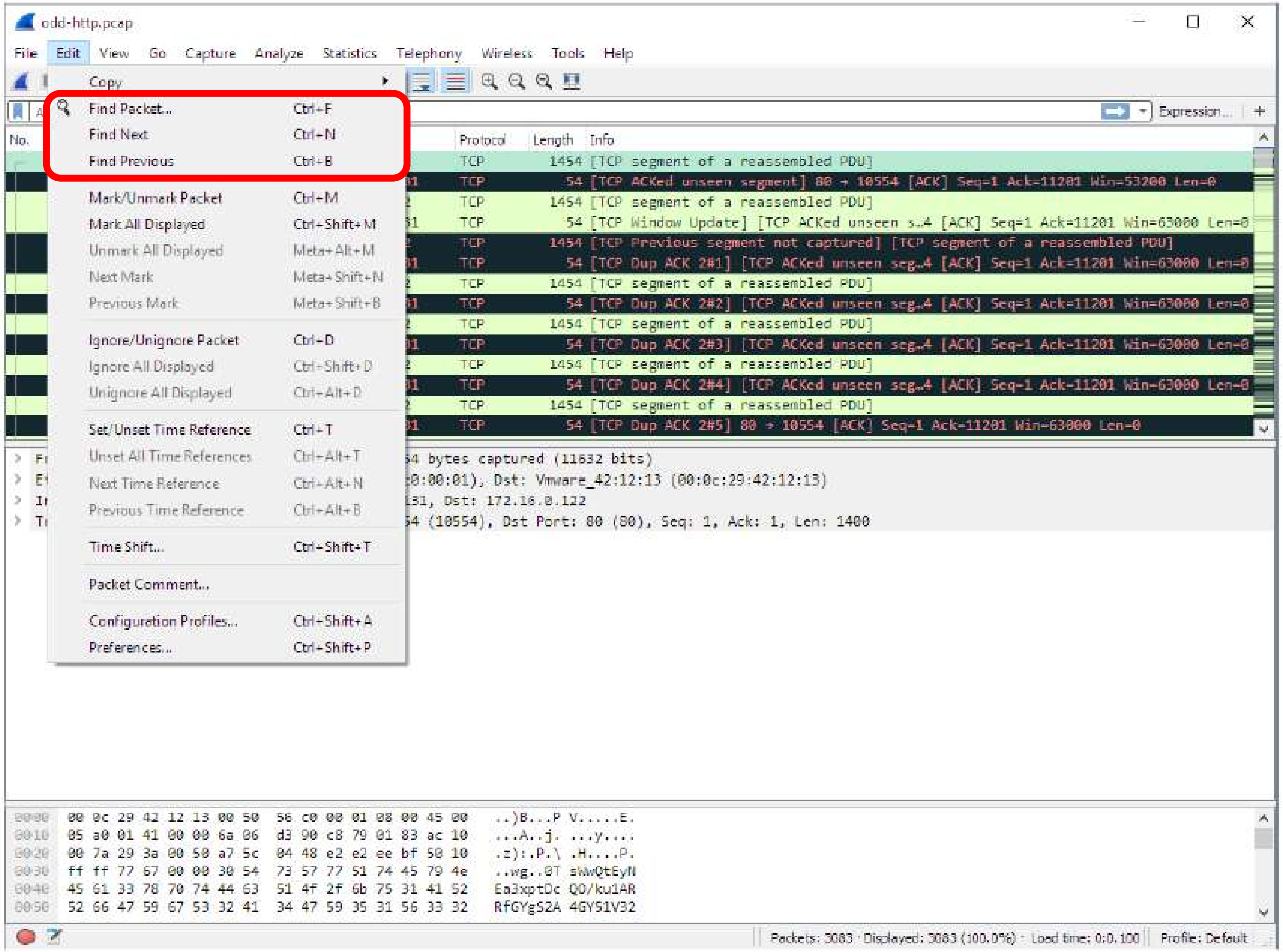
ip.src == 184.168.27.206 and ip.dst ==192.168.0.35

```
No.  Time                        Source          Destination   Protocol Length Info
  40 2015-10-14 00:38:53.738599 184.168.27.206  192.168.0.35  HTTP      421 HTTP/1.1 200 OK  (JPEG JFIF image)
  45 2015-10-14 00:38:53.799096 184.168.27.206  192.168.0.35  HTTP      813 HTTP/1.1 200 OK  (JPEG JFIF image)
  49 2015-10-14 00:38:53.804074 184.168.27.206  192.168.0.35  HTTP      730 HTTP/1.1 200 OK  (JPEG JFIF image)
  56 2015-10-14 00:38:53.815059 184.168.27.206  192.168.0.35  HTTP      863 HTTP/1.1 200 OK  (JPEG JFIF image)
  73 2015-10-14 00:38:53.858437 184.168.27.206  192.168.0.35  HTTP     1071 HTTP/1.1 200 OK  (GIF89a)
 103 2015-10-14 00:38:53.932614 184.168.27.206  192.168.0.35  HTTP      870 HTTP/1.1 200 OK  (JPEG JFIF image)
 120 2015-10-14 00:38:53.969572 184.168.27.206  192.168.0.35  HTTP      981 HTTP/1.1 200 OK  (JPEG JFIF image)
 132 2015-10-14 00:38:53.981064 184.168.27.206  192.168.0.35  HTTP     1307 HTTP/1.1 200 OK  (GIF89a)
 147 2015-10-14 00:38:54.048791 184.168.27.206  192.168.0.35  HTTP      842 HTTP/1.1 200 OK  (JPEG JFIF image)
 181 2015-10-14 00:38:54.073072 184.168.27.206  192.168.0.35  HTTP      126 HTTP/1.1 200 OK  (JPEG JFIF image)
 185 2015-10-14 00:38:54.111129 184.168.27.206  192.168.0.35  HTTP      608 HTTP/1.1 200 OK  (JPEG JFIF image)
 188 2015-10-14 00:38:54.117576 184.168.27.206  192.168.0.35  HTTP      821 [TCP Previous segment not captured] Continuation
```

```
> Frame 40: 421 bytes on wire (3368 bits), 421 bytes captured (3368 bits) on interface 0
> Ethernet II, Src: ArrisGro_0f:ca:07 (d4:05:98:0f:ca:07), Dst: Vmware_37:07:ed (00:0c:29:37:07:ed)
> Internet Protocol Version 4, Src: 184.168.27.206, Dst: 192.168.0.35
> Transmission Control Protocol, Src Port: 80, Dst Port: 1237, Seq: 1461, Ack: 362, Len: 367
> [2 Reassembled TCP Segments (1827 bytes): #39(1460), #40(367)]
> Hypertext Transfer Protocol
> JPEG File Interchange Format
```

```
0000  00 0c 29 37 07 ed d4 05  98 0f ca 07 08 00 45 00   ..)7.... ......E.
0010  01 97 77 b2 40 00 71 06  fb 6c b8 a8 1b ce c0 a8   ..w.@.q. .l......
0020  00 23 00 50 04 d5 ce 4a  a9 a9 ff 0f e2 9d 50 18   .#.P...J ......P.
0030  fa f0 8c ca 00 00 0a 42  da b2 bb d7 4e 1e 3b 72   .......B ....N.;r
0040  85 c1 20 26 77 2b a8 75  84 a5 01 1b a5 bf 22 ce   .. &w+.u ......".
0050  c8 09 1a 98 4e 8e ab ea  4d 48 ed 80 5e d1 13 59   ....N... MH..^..Y
0060  1a 62 b7 8d 34 93 70 42  a6 a0 4a 72 1b c5 21 72   .b..4.pB ..Jr..!r
0070  f9 a0 35 95 1e 59 60 fa  b5 2e ad 46 a8 52 d3 5e   ..5..Y`. ...F.R.^
0080  9f 5b 76 6a 93 f4 cc 63  cc 5e 98 a4 2e dc 87 01   .[vj...c .^......
0090  bc 9a 81 b3 28 94 c4 10  12 88 4c 25 00 c2 5c b7   ....(... ..L%..\.
00a0  c3 b8 28 cf 14 a2 15 d9  97 7e 09 15 d2 ef df 3a   ..(..... .~.....:
00b0  a8 ac 62 a0 27 14 cb b4  76 a2 a6 02 94 54 3c 80   ..b.'... v....T<.
00c0  06 56 8c 04 9f 75 cd 00  dd 73 40 61 72 d2 69 18   .V...u.. .s@ar.i.
```

Useful Wireshark Tips: Edit Menu


odd-http.pcap
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Meta+Alt+M
Next Mark Meta+Shift+N
Previous Mark Meta+Shift+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comment...
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P
Expression...
+
No.
Protocol
Length
Info

```
     TCP    1454 [TCP segment of a reassembled PDU]
31   TCP      54 [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=53200 Len=0
2    TCP    1454 [TCP segment of a reassembled PDU]
31   TCP      54 [TCP Window Update] [TCP ACKed unseen s…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
2    TCP    1454 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]
31   TCP      54 [TCP Dup ACK 2#1] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
2    TCP    1454 [TCP segment of a reassembled PDU]
31   TCP      54 [TCP Dup ACK 2#2] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
2    TCP    1454 [TCP segment of a reassembled PDU]
31   TCP      54 [TCP Dup ACK 2#3] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
2    TCP    1454 [TCP segment of a reassembled PDU]
31   TCP      54 [TCP Dup ACK 2#4] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
2    TCP    1454 [TCP segment of a reassembled PDU]
31   TCP      54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
```

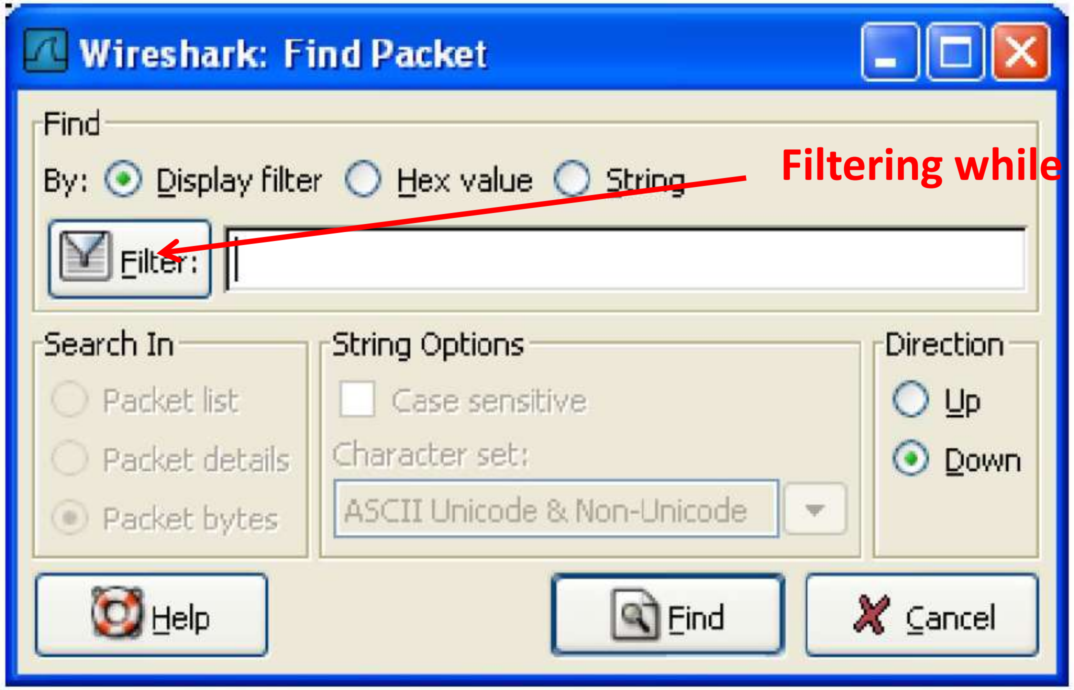
```
> Fr 54 bytes captured (11632 bits)
> Et :0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
> Ir 131, Dst: 172.16.0.122
> Tr 54 (10554), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1400
```

```
0000  00 0c 29 42 12 13 00 50  56 c0 00 01 08 00 45 00   ..)B...P V.....E.
0010  05 a0 01 41 00 00 6a 06  d3 90 c8 79 01 83 ac 10   ...A..j. ...y....
0020  00 7a 29 3a 00 50 a7 5c  04 48 e2 e2 ee bf 50 10   .z):.P.\ .H....P.
0030  ff ff 77 67 00 00 30 54  73 57 77 51 74 45 79 4e   ..wg..0T sWwQtEyN
0040  45 61 33 78 70 74 44 63  51 4f 2f 6b 75 31 41 52   Ea3xptDc QO/ku1AR
0050  52 66 47 59 67 53 32 41  34 47 59 35 31 56 33 32   RfGYgS2A 4GY51V32
```

Packets: 3083 · Displayed: 3083 (100.0%) · Load time: 0:0.100 | Profile: Default

Source: Wireshark User's Guide

Useful Wireshark Tips: Find Packet



By: ● Display filter ○ Hex value ○ String

Search In: ○ Packet list ○ Packet details ● Packet bytes

String Options: □ Case sensitive

Character set: ASCII Unicode & Non-Unicode

Direction: ○ Up ● Down

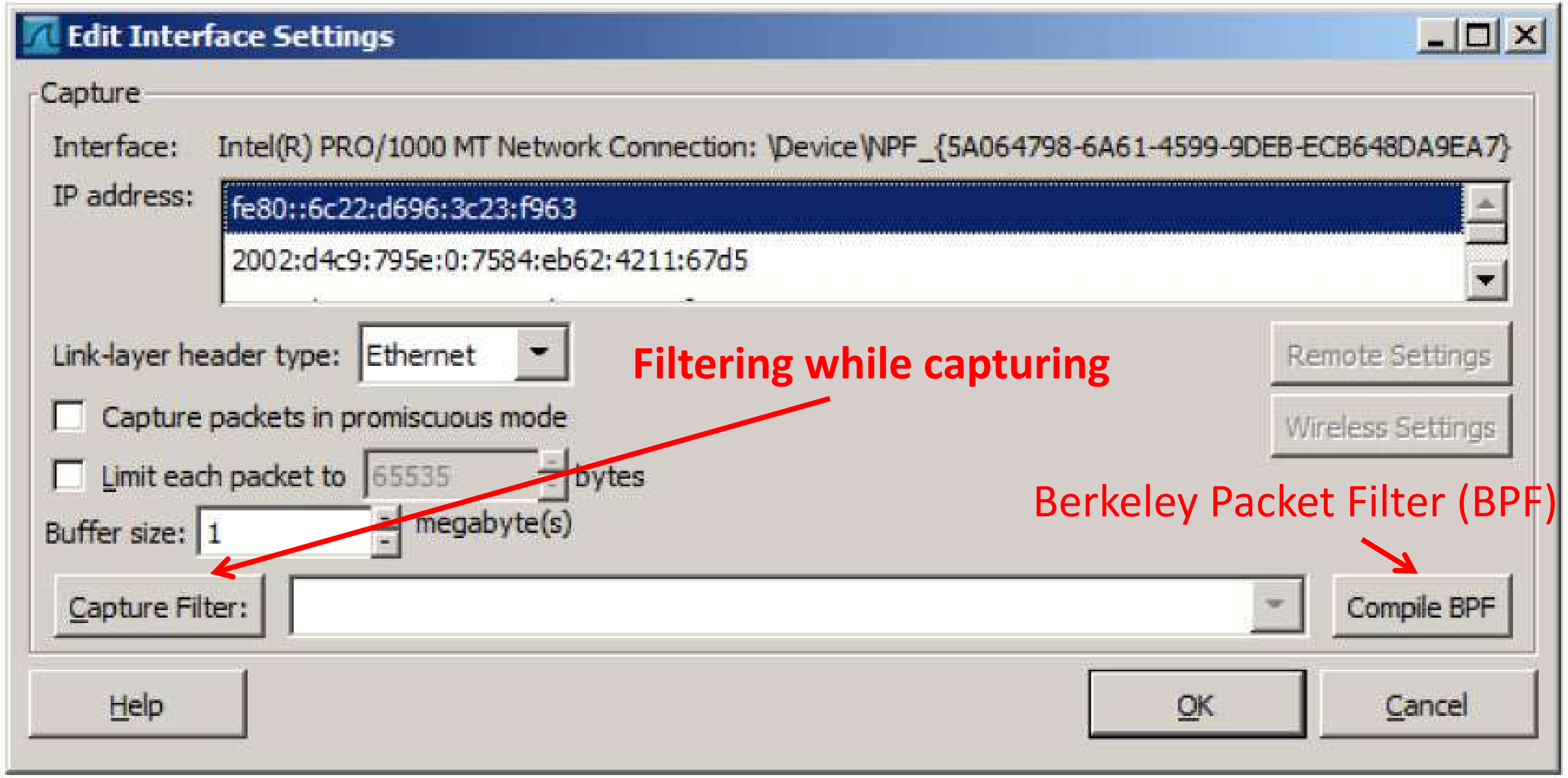
Filtering while displaying

Figure 64. The "Find Packet" dialog box

Source: Wireshark User's Guide

Useful Wireshark Tips

Interface setting:



Edit Interface Settings

Capture

Interface: Intel(R) PRO/1000 MT Network Connection: \Device\NPF_{5A064798-6A61-4599-9DEB-ECB648DA9EA7}

IP address: fe80::6c22:d696:3c23:f963
2002:d4c9:795e:0:7584:eb62:4211:67d5

Link-layer header type: Ethernet

□ Capture packets in promiscuous mode

□ Limit each packet to 65535 bytes

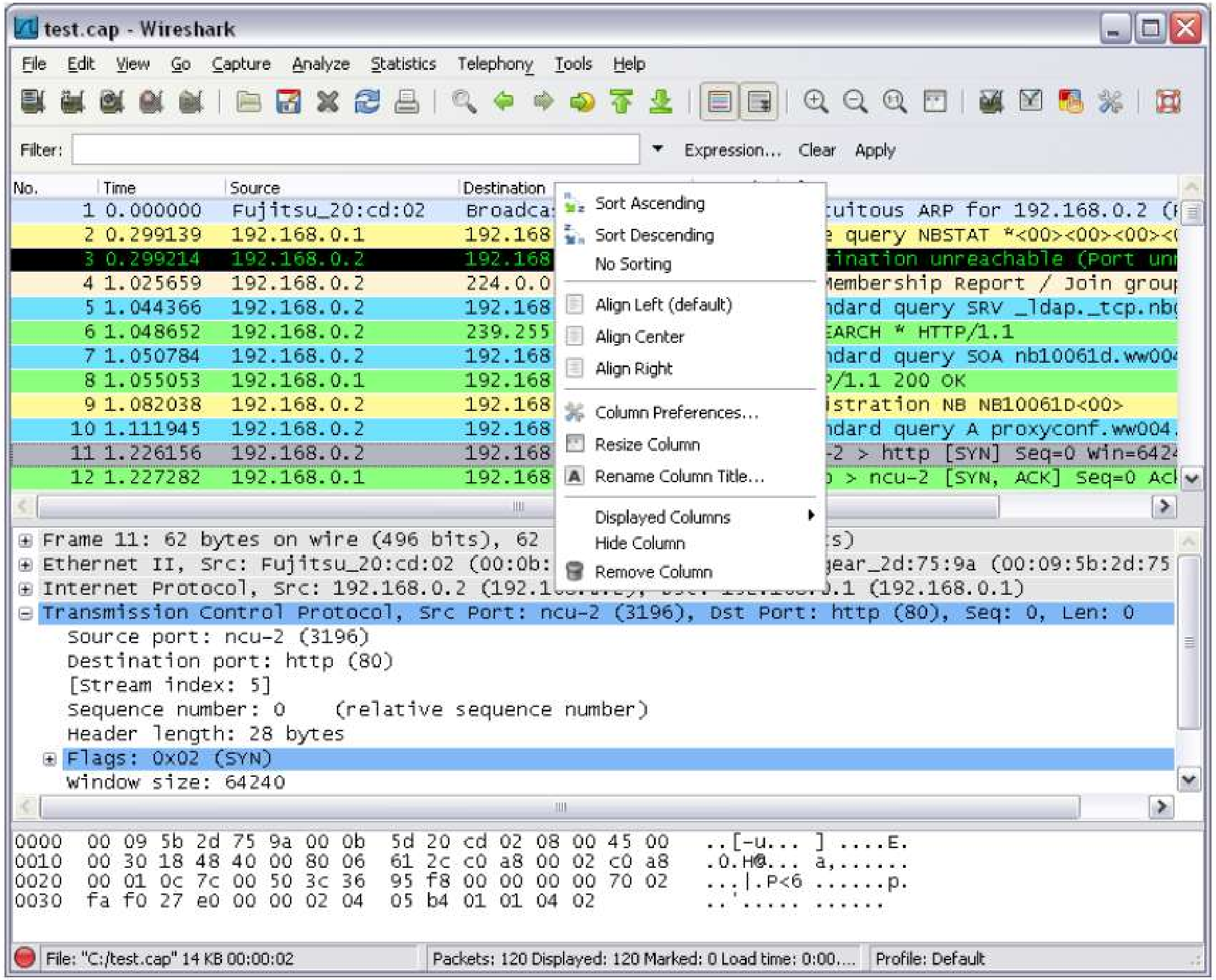
Buffer size: 1 megabyte(s)

Filtering while capturing

Berkeley Packet Filter (BPF) syntax

Source: Wireshark User's Guide

Useful Wireshark Tips: Popup Menu 1



```
No.   Time        Source              Destination
  1 0.000000    Fujitsu_20:cd:02    Broadca:        tuitous ARP for 192.168.0.2 (R
  2 0.299139    192.168.0.1         192.168         e query NBSTAT *<00><00><00><0
  3 0.299214    192.168.0.2         192.168         tination unreachable (Port unr
  4 1.025659    192.168.0.2         224.0.0         Membership Report / Join group
  5 1.044366    192.168.0.2         192.168         ndard query SRV _ldap._tcp.nb
  6 1.048652    192.168.0.2         239.255         EARCH * HTTP/1.1
  7 1.050784    192.168.0.2         192.168         ndard query SOA nb10061d.ww004
  8 1.055053    192.168.0.1         192.168         P/1.1 200 OK
  9 1.082038    192.168.0.2         192.168         istration NB NB10061D<00>
 10 1.111945    192.168.0.2         192.168         ndard query A proxyconf.ww004.
 11 1.226156    192.168.0.2         192.168         -2 > http [SYN] Seq=0 Win=6424
 12 1.227282    192.168.0.1         192.168         p > ncu-2 [SYN, ACK] Seq=0 Ack
```

```
⊞ Frame 11: 62 bytes on wire (496 bits), 62                    s)
⊞ Ethernet II, Src: Fujitsu_20:cd:02 (00:0b:                   gear_2d:75:9a (00:09:5b:2d:75
⊞ Internet Protocol, Src: 192.168.0.2 (192.1                   0.1 (192.168.0.1)
⊟ Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0
    Source port: ncu-2 (3196)
    Destination port: http (80)
    [Stream index: 5]
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size: 64240
```

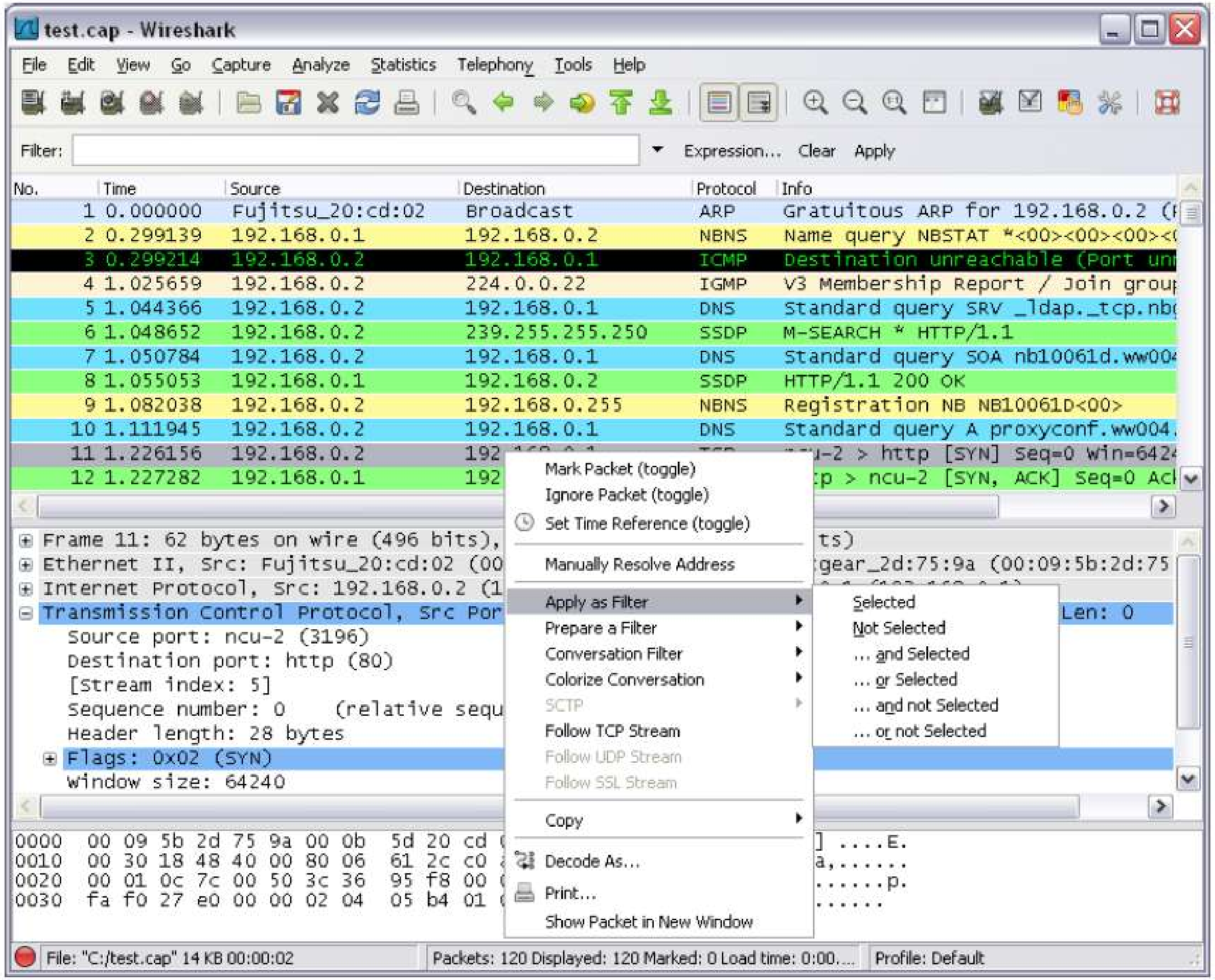
```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

File: "C:/test.cap" 14 KB 00:00:02 | Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00.... | Profile: Default

Figure 58. Pop-up menu of the "Packet List" column header

Source: Wireshark User's Guide

Useful Wireshark Tips: Popup Menu 2



```
No.   Time        Source              Destination       Protocol  Info
    1 0.000000    Fujitsu_20:cd:02    Broadcast         ARP       Gratuitous ARP for 192.168.0.2 (R
    2 0.299139    192.168.0.1         192.168.0.2       NBNS      Name query NBSTAT *<00><00><00><0
    3 0.299214    192.168.0.2         192.168.0.1       ICMP      Destination unreachable (Port unr
    4 1.025659    192.168.0.2         224.0.0.22        IGMP      V3 Membership Report / Join group
    5 1.044366    192.168.0.2         192.168.0.1       DNS       Standard query SRV _ldap._tcp.nbd
    6 1.048652    192.168.0.2         239.255.255.250   SSDP      M-SEARCH * HTTP/1.1
    7 1.050784    192.168.0.2         192.168.0.1       DNS       Standard query SOA nb10061d.ww004
    8 1.055053    192.168.0.1         192.168.0.2       SSDP      HTTP/1.1 200 OK
    9 1.082038    192.168.0.2         192.168.0.255     NBNS      Registration NB NB10061D<00>
   10 1.111945    192.168.0.2         192.168.0.1       DNS       Standard query A proxyconf.ww004.
   11 1.226156    192.168.0.2         192                         u-2 > http [SYN] Seq=0 Win=6424
   12 1.227282    192.168.0.1         192                         tp > ncu-2 [SYN, ACK] Seq=0 Ack
```

```
⊞ Frame 11: 62 bytes on wire (496 bits),                              ts)
⊞ Ethernet II, Src: Fujitsu_20:cd:02 (00                              gear_2d:75:9a (00:09:5b:2d:75
⊞ Internet Protocol, Src: 192.168.0.2 (1
⊟ Transmission Control Protocol, Src Por                                                 Len: 0
    Source port: ncu-2 (3196)
    Destination port: http (80)
    [Stream index: 5]
    Sequence number: 0    (relative sequ
    Header length: 28 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size: 64240
```

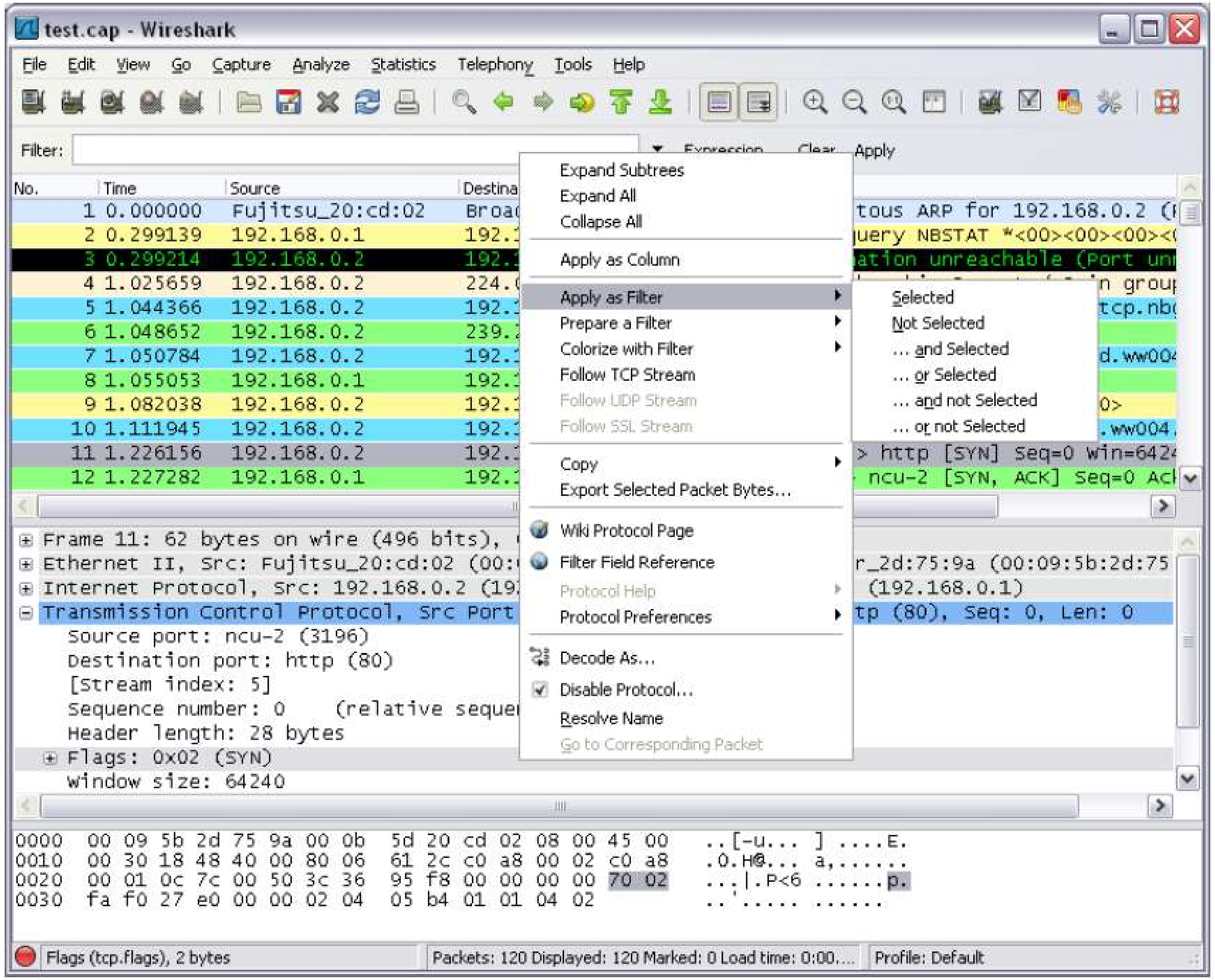
```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd                 ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0                 a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00                 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01                 .....
```

File: "C:/test.cap" 14 KB 00:00:02 | Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00.... | Profile: Default

Figure 59. Pop-up menu of the "Packet List" pane

Source: Wireshark User's Guide

Useful Wireshark Tips: Popup Menu 3



```
No.   Time      Source             Destina
 1 0.000000  Fujitsu_20:cd:02   Broa       tous ARP for 192.168.0.2 (
 2 0.299139  192.168.0.1        192.1      uery NBSTAT *<00><00><00><
 3 0.299214  192.168.0.2        192.1      ation unreachable (Port un
 4 1.025659  192.168.0.2        224.0      n grou
 5 1.044366  192.168.0.2        192.1      tcp.nb
 6 1.048652  192.168.0.2        239.2
 7 1.050784  192.168.0.2        192.1      d.ww00
 8 1.055053  192.168.0.1        192.1
 9 1.082038  192.168.0.2        192.1      0>
10 1.111945  192.168.0.2        192.1      .ww004.
11 1.226156  192.168.0.2        192.1      > http [SYN] Seq=0 Win=642
12 1.227282  192.168.0.1        192.1      ncu-2 [SYN, ACK] Seq=0 Ack
```

```
⊞ Frame 11: 62 bytes on wire (496 bits),
⊞ Ethernet II, Src: Fujitsu_20:cd:02 (00:      r_2d:75:9a (00:09:5b:2d:75
⊞ Internet Protocol, Src: 192.168.0.2 (19       (192.168.0.1)
⊟ Transmission Control Protocol, Src Port      tp (80), Seq: 0, Len: 0
    Source port: ncu-2 (3196)
    Destination port: http (80)
    [Stream index: 5]
    Sequence number: 0    (relative seque
    Header length: 28 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size: 64240
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

Flags (tcp.flags), 2 bytes | Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00.... | Profile: Default

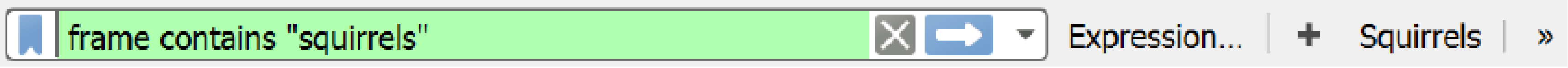
Figure 60. Pop-up menu of the "Packet Details" pane

Source: Wireshark User's Guide

Review

Useful Wireshark Tips: Display Filter

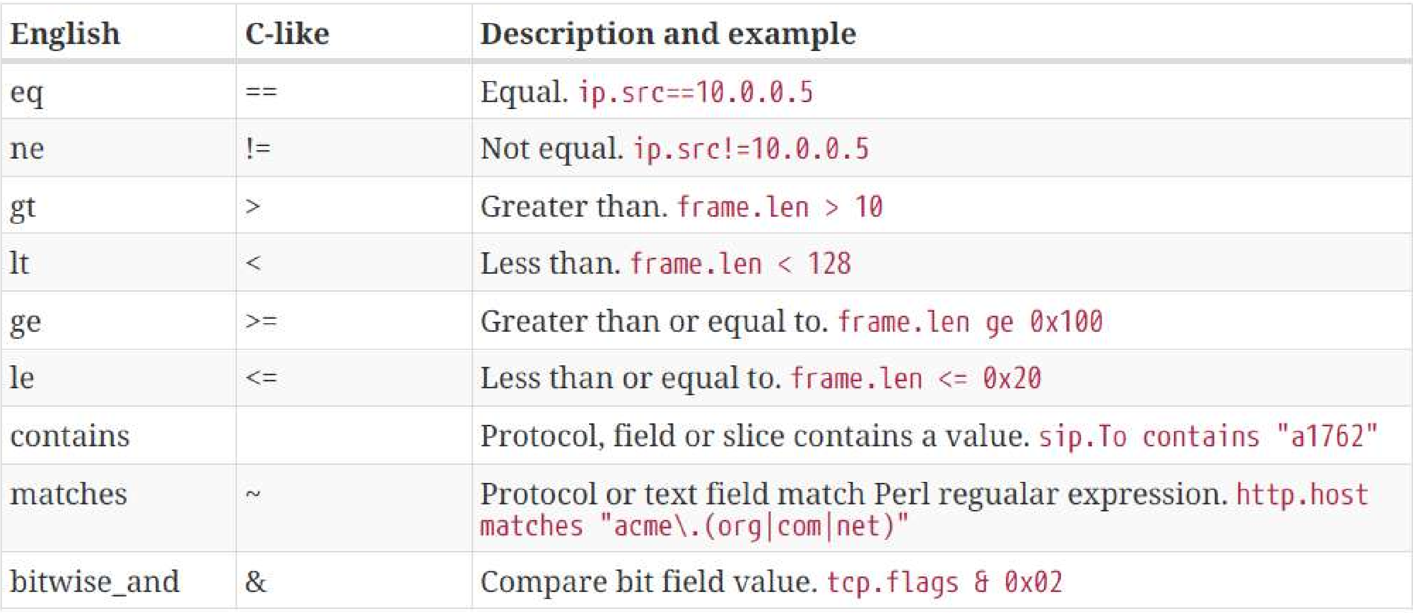
You need to specify a good display filter:



```
frame contains "squirrels"
```

Filter comparison operators

Table 20. Display Filter comparison operators

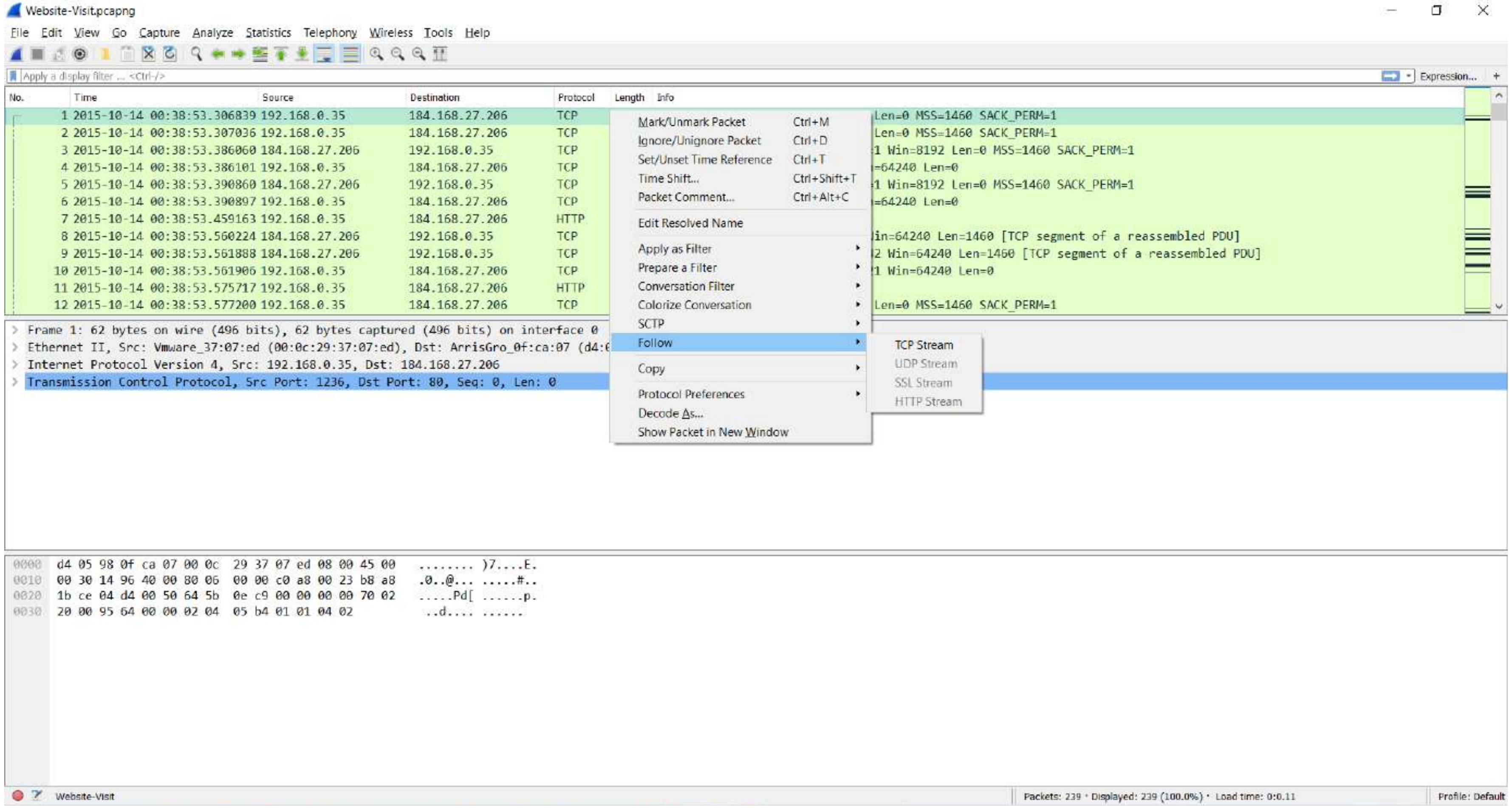


English	C-like	Description and example
eq	==	Equal. `ip.src==10.0.0.5`
ne	!=	Not equal. `ip.src!=10.0.0.5`
gt	>	Greater than. `frame.len > 10`
lt	<	Less than. `frame.len < 128`
ge	>=	Greater than or equal to. `frame.len ge 0x100`
le	<=	Less than or equal to. `frame.len <= 0x20`
contains		Protocol, field or slice contains a value. `sip.To contains "a1762"`
matches	~	Protocol or text field match Perl regualar expression. `http.host matches "acme\.(org|com|net)"`
bitwise_and	&	Compare bit field value. `tcp.flags & 0x02`

Source: Wireshark User's Guide

Review

Useful Wireshark Tips: Follow TCP Stream


Website-Visit.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
HTTP Stream
Website-Visit
Profile: Default

```
No.     Time                       Source          Destination     Protocol  Length  Info
  1 2015-10-14 00:38:53.306839 192.168.0.35    184.168.27.206  TCP       Len=0 MSS=1460 SACK_PERM=1
  2 2015-10-14 00:38:53.307036 192.168.0.35    184.168.27.206  TCP       Len=0 MSS=1460 SACK_PERM=1
  3 2015-10-14 00:38:53.386060 184.168.27.206  192.168.0.35    TCP       1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
  4 2015-10-14 00:38:53.386101 192.168.0.35    184.168.27.206  TCP       =64240 Len=0
  5 2015-10-14 00:38:53.390860 184.168.27.206  192.168.0.35    TCP       1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
  6 2015-10-14 00:38:53.390897 192.168.0.35    184.168.27.206  TCP       =64240 Len=0
  7 2015-10-14 00:38:53.459163 192.168.0.35    184.168.27.206  HTTP
  8 2015-10-14 00:38:53.560224 184.168.27.206  192.168.0.35    TCP       in=64240 Len=1460 [TCP segment of a reassembled PDU]
  9 2015-10-14 00:38:53.561888 184.168.27.206  192.168.0.35    TCP       2 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
 10 2015-10-14 00:38:53.561906 192.168.0.35    184.168.27.206  TCP       1 Win=64240 Len=0
 11 2015-10-14 00:38:53.575717 192.168.0.35    184.168.27.206  HTTP
 12 2015-10-14 00:38:53.577200 192.168.0.35    184.168.27.206  TCP       Len=0 MSS=1460 SACK_PERM=1
```

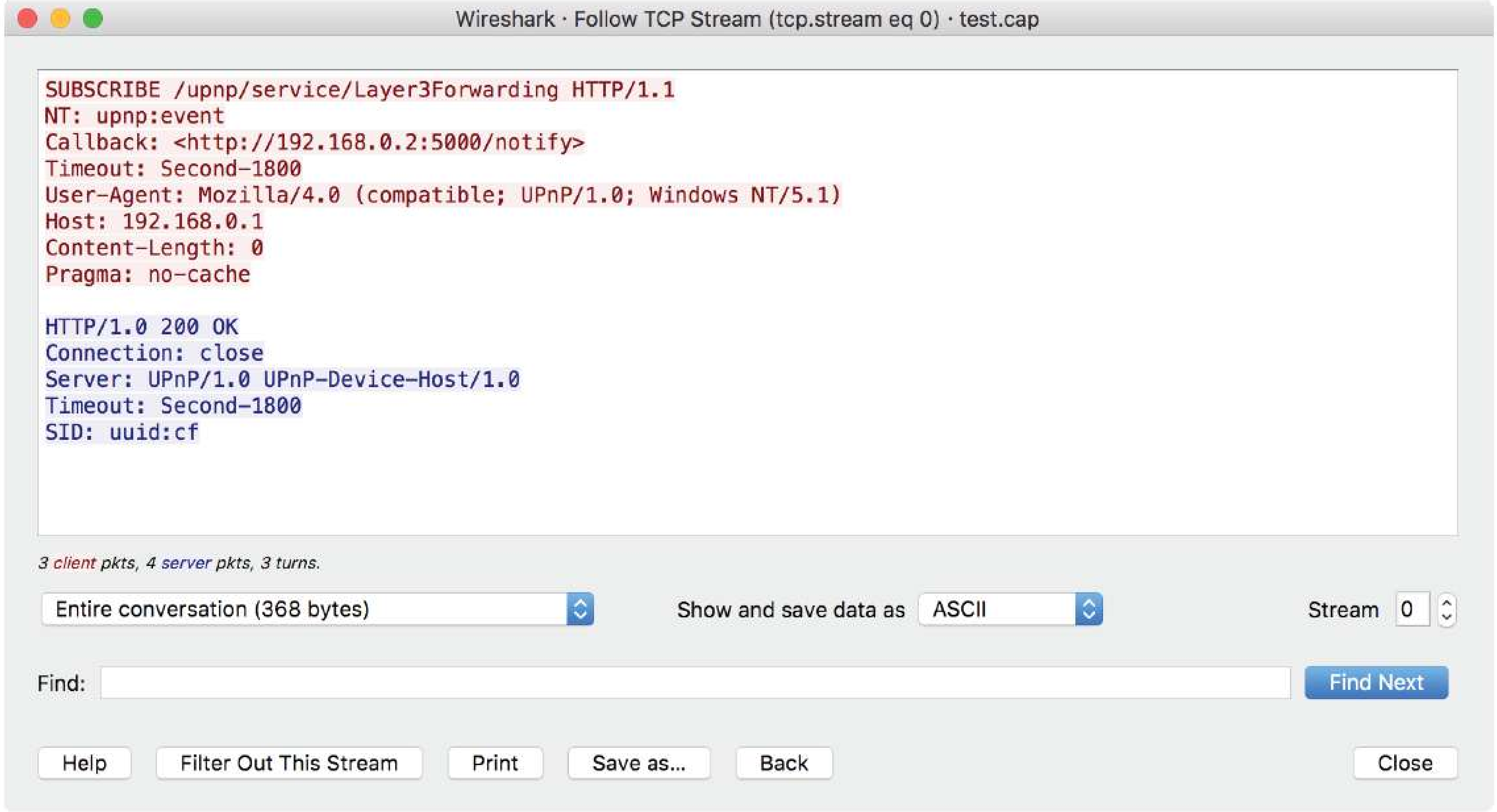
```
> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
> Ethernet II, Src: Vmware_37:07:ed (00:0c:29:37:07:ed), Dst: ArrisGro_0f:ca:07 (d4:(
> Internet Protocol Version 4, Src: 192.168.0.35, Dst: 184.168.27.206
> Transmission Control Protocol, Src Port: 1236, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  d4 05 98 0f ca 07 00 0c  29 37 07 ed 08 00 45 00   ........ )7....E.
0010  00 30 14 96 40 00 80 06  00 00 c0 a8 00 23 b8 a8   .0..@... .....#..
0020  1b ce 04 d4 00 50 64 5b  0e c9 00 00 00 00 70 02   .....Pd[ ......p.
0030  20 00 95 64 00 00 02 04  05 b4 01 01 04 02          ..d.... ......
```

Packets: 239 · Displayed: 239 (100.0%) · Load time: 0:0.11

Review

Useful Wireshark Tips: Follow TCP Stream



Wireshark · Follow TCP Stream (tcp.stream eq 0) · test.cap

```
SUBSCRIBE /upnp/service/Layer3Forwarding HTTP/1.1
NT: upnp:event
Callback: <http://192.168.0.2:5000/notify>
Timeout: Second-1800
User-Agent: Mozilla/4.0 (compatible; UPnP/1.0; Windows NT/5.1)
Host: 192.168.0.1
Content-Length: 0
Pragma: no-cache

HTTP/1.0 200 OK
Connection: close
Server: UPnP/1.0 UPnP-Device-Host/1.0
Timeout: Second-1800
SID: uuid:cf
```

3 client pkts, 4 server pkts, 3 turns.

Entire conversation (368 bytes)

Show and save data as: ASCII

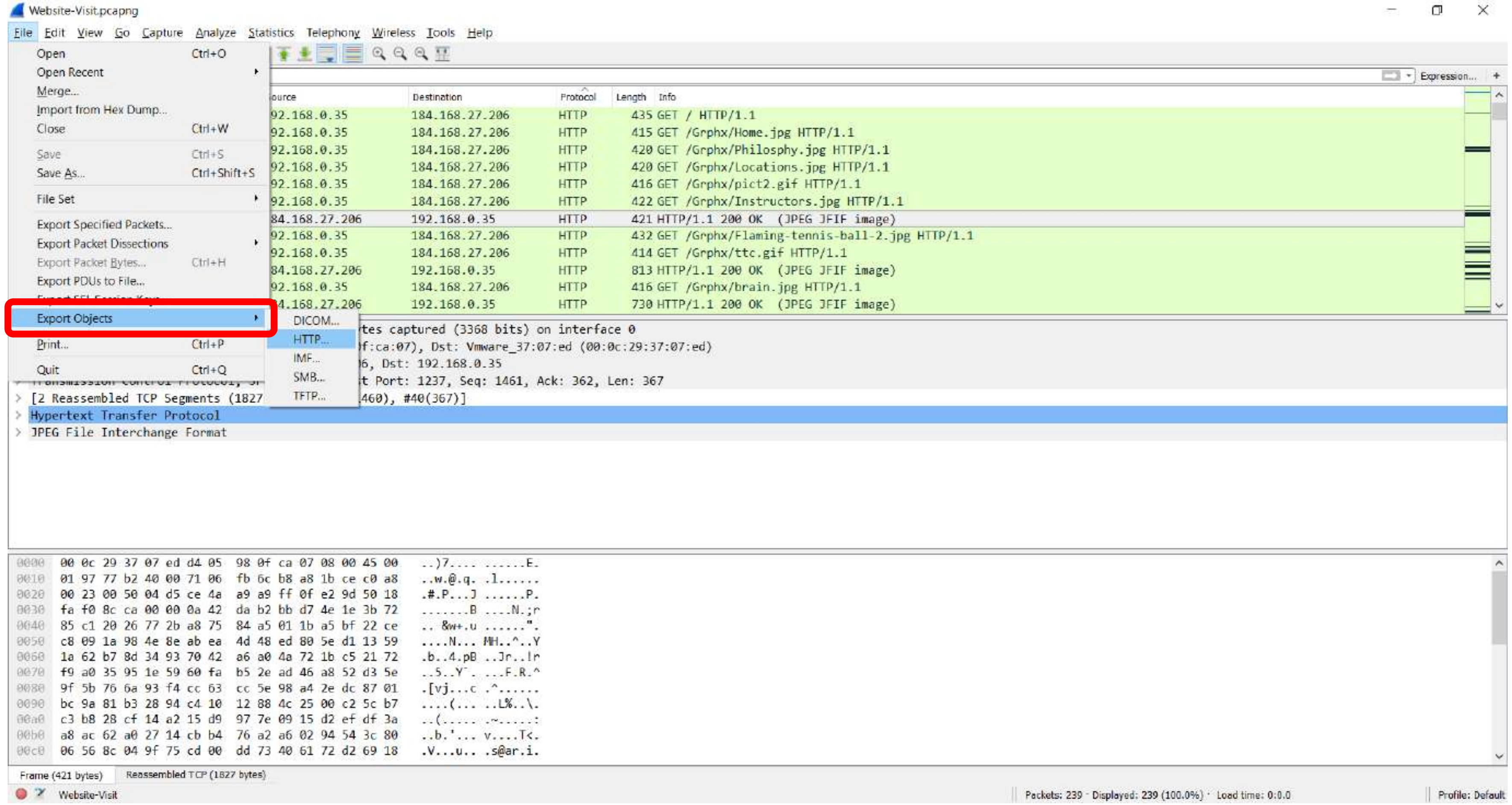
Stream: 0

Find:

Figure 67. The “Follow TCP Stream” dialog box

Source: Wireshark User's Guide

Useful Wireshark Tips: Export Object



```
ource            Destination      Protocol  Length Info
92.168.0.35      184.168.27.206   HTTP       435 GET / HTTP/1.1
92.168.0.35      184.168.27.206   HTTP       415 GET /Grphx/Home.jpg HTTP/1.1
92.168.0.35      184.168.27.206   HTTP       420 GET /Grphx/Philosphy.jpg HTTP/1.1
92.168.0.35      184.168.27.206   HTTP       420 GET /Grphx/Locations.jpg HTTP/1.1
92.168.0.35      184.168.27.206   HTTP       416 GET /Grphx/pict2.gif HTTP/1.1
92.168.0.35      184.168.27.206   HTTP       422 GET /Grphx/Instructors.jpg HTTP/1.1
84.168.27.206    192.168.0.35     HTTP       421 HTTP/1.1 200 OK  (JPEG JFIF image)
92.168.0.35      184.168.27.206   HTTP       432 GET /Grphx/Flaming-tennis-ball-2.jpg HTTP/1.1
92.168.0.35      184.168.27.206   HTTP       414 GET /Grphx/ttc.gif HTTP/1.1
84.168.27.206    192.168.0.35     HTTP       813 HTTP/1.1 200 OK  (JPEG JFIF image)
92.168.0.35      184.168.27.206   HTTP       416 GET /Grphx/brain.jpg HTTP/1.1
4.168.27.206     192.168.0.35     HTTP       730 HTTP/1.1 200 OK  (JPEG JFIF image)
```

```
tes captured (3368 bits) on interface 0
f:ca:07), Dst: Vmware_37:07:ed (00:0c:29:37:07:ed)
6, Dst: 192.168.0.35
t Port: 1237, Seq: 1461, Ack: 362, Len: 367
> [2 Reassembled TCP Segments (1827 460), #40(367)]
> Hypertext Transfer Protocol
> JPEG File Interchange Format
```

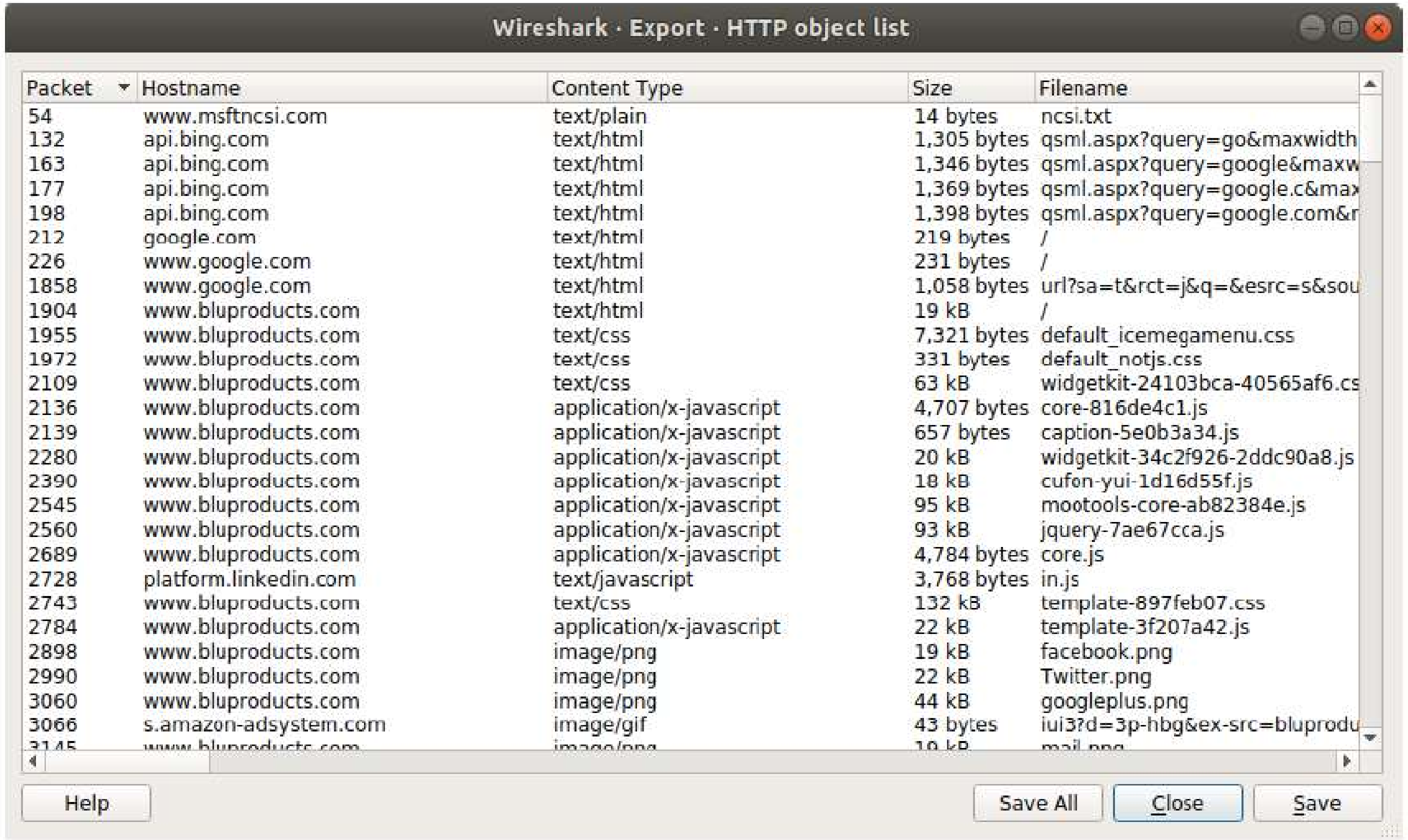
```
0000  00 0c 29 37 07 ed d4 05  98 0f ca 07 08 00 45 00   ..)7.... ......E.
0010  01 97 77 b2 40 00 71 06  fb 6c b8 a8 1b ce c0 a8   ..w.@.q. .l......
0020  00 23 00 50 04 d5 ce 4a  a9 a9 ff 0f e2 9d 50 18   .#.P...J ......P.
0030  fa f0 8c ca 00 00 0a 42  da b2 bb d7 4e 1e 3b 72   .......B ....N.;r
0040  85 c1 20 26 77 2b a8 75  84 a5 01 1b a5 bf 22 ce   .. &w+.u ......".
0050  c8 09 1a 98 4e 8e ab ea  4d 48 ed 80 5e d1 13 59   ....N... MH..^..Y
0060  1a 62 b7 8d 34 93 70 42  a6 a0 4a 72 1b c5 21 72   .b..4.pB ..Jr..!r
0070  f9 a0 35 95 1e 59 60 fa  b5 2e ad 46 a8 52 d3 5e   ..5..Y`. ...F.R.^
0080  9f 5b 76 6a 93 f4 cc 63  cc 5e 98 a4 2e dc 87 01   .[vj...c .^......
0090  bc 9a 81 b3 28 94 c4 10  12 88 4c 25 00 c2 5c b7   ....(... ..L%..\.
00a0  c3 b8 28 cf 14 a2 15 d9  97 7e 09 15 d2 ef df 3a   ..(..... .~.....:
00b0  a8 ac 62 a0 27 14 cb b4  76 a2 a6 02 94 54 3c 80   ..b.'... v....T<.
00c0  06 56 8c 04 9f 75 cd 00  dd 73 40 61 72 d2 69 18   .V...u.. .s@ar.i.
```

Frame (421 bytes) | Reassembled TCP (1827 bytes)

Website-Visit | Packets: 239 · Displayed: 239 (100.0%) · Load time: 0:0.0 | Profile: Default

Useful Wireshark Tips: Export Object

- Export HTTP objects:



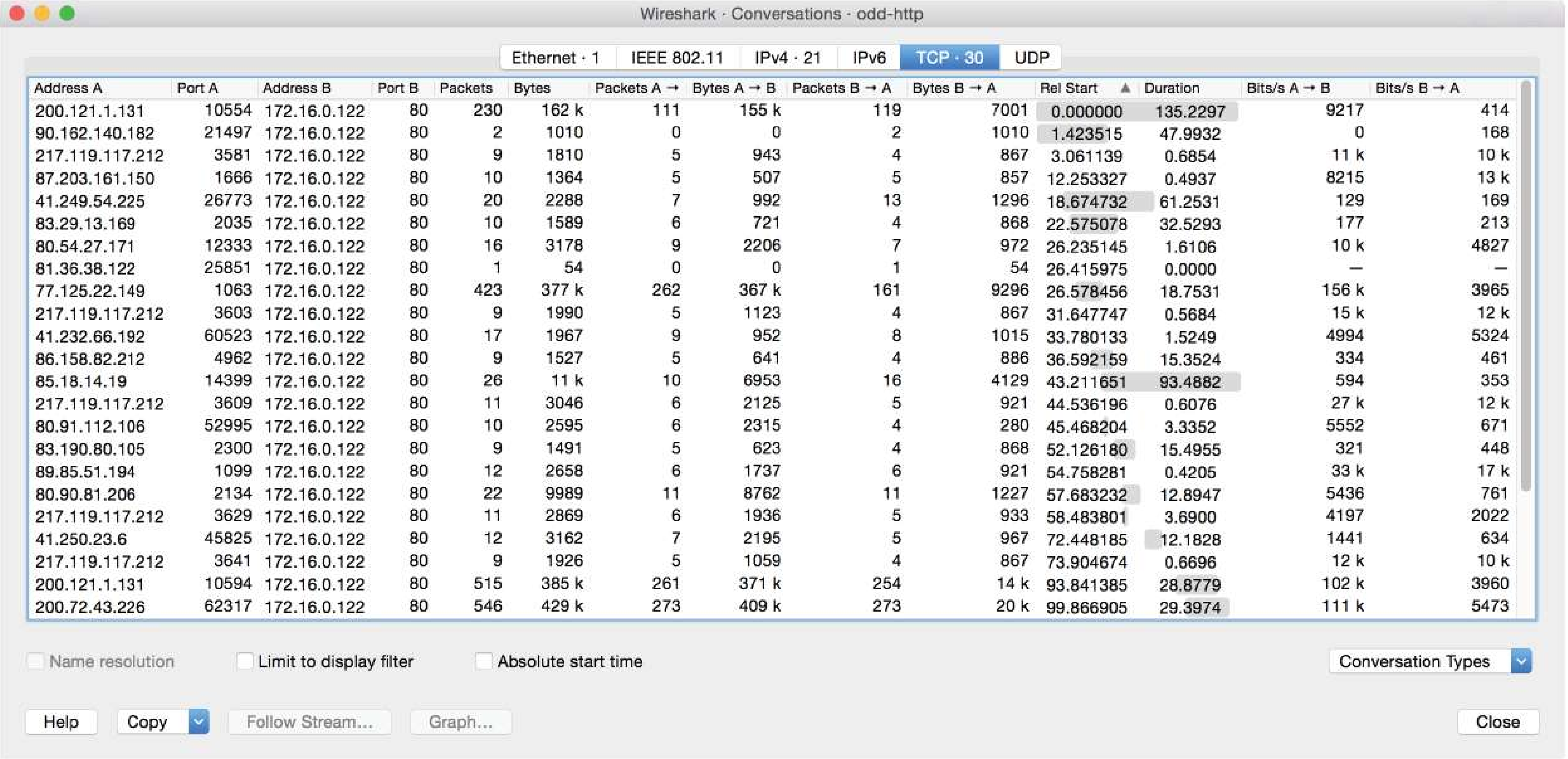
Packet	Hostname	Content Type	Size	Filename
54	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
132	api.bing.com	text/html	1,305 bytes	qsml.aspx?query=go&maxwidth
163	api.bing.com	text/html	1,346 bytes	qsml.aspx?query=google&maxw
177	api.bing.com	text/html	1,369 bytes	qsml.aspx?query=google.c&max
198	api.bing.com	text/html	1,398 bytes	qsml.aspx?query=google.com&r
212	google.com	text/html	219 bytes	/
226	www.google.com	text/html	231 bytes	/
1858	www.google.com	text/html	1,058 bytes	url?sa=t&rct=j&q=&esrc=s&sou
1904	www.bluproducts.com	text/html	19 kB	/
1955	www.bluproducts.com	text/css	7,321 bytes	default_icemegamenu.css
1972	www.bluproducts.com	text/css	331 bytes	default_notjs.css
2109	www.bluproducts.com	text/css	63 kB	widgetkit-24103bca-40565af6.cs
2136	www.bluproducts.com	application/x-javascript	4,707 bytes	core-816de4c1.js
2139	www.bluproducts.com	application/x-javascript	657 bytes	caption-5e0b3a34.js
2280	www.bluproducts.com	application/x-javascript	20 kB	widgetkit-34c2f926-2ddc90a8.js
2390	www.bluproducts.com	application/x-javascript	18 kB	cufon-yui-1d16d55f.js
2545	www.bluproducts.com	application/x-javascript	95 kB	mootools-core-ab82384e.js
2560	www.bluproducts.com	application/x-javascript	93 kB	jquery-7ae67cca.js
2689	www.bluproducts.com	application/x-javascript	4,784 bytes	core.js
2728	platform.linkedin.com	text/javascript	3,768 bytes	in.js
2743	www.bluproducts.com	text/css	132 kB	template-897feb07.css
2784	www.bluproducts.com	application/x-javascript	22 kB	template-3f207a42.js
2898	www.bluproducts.com	image/png	19 kB	facebook.png
2990	www.bluproducts.com	image/png	22 kB	Twitter.png
3060	www.bluproducts.com	image/png	44 kB	googleplus.png
3066	s.amazon-adsystem.com	image/gif	43 bytes	iui3?d=3p-hbg&ex-src=bluprodu
3145	www.bluproducts.com	image/png	10 kB	mail.png

Figure 52. The "Export Objects" dialog box

Source: Wireshark User's Guide

Review

Useful Wireshark Tips: Statistics



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A →	Bytes A → B	Packets B → A	Bytes B → A	Rel Start ▲	Duration	Bits/s A → B	Bits/s B → A
200.121.1.131	10554	172.16.0.122	80	230	162 k	111	155 k	119	7001	0.000000	135.2297	9217	414
90.162.140.182	21497	172.16.0.122	80	2	1010	0	0	2	1010	1.423515	47.9932	0	168
217.119.117.212	3581	172.16.0.122	80	9	1810	5	943	4	867	3.061139	0.6854	11 k	10 k
87.203.161.150	1666	172.16.0.122	80	10	1364	5	507	5	857	12.253327	0.4937	8215	13 k
41.249.54.225	26773	172.16.0.122	80	20	2288	7	992	13	1296	18.674732	61.2531	129	169
83.29.13.169	2035	172.16.0.122	80	10	1589	6	721	4	868	22.575078	32.5293	177	213
80.54.27.171	12333	172.16.0.122	80	16	3178	9	2206	7	972	26.235145	1.6106	10 k	4827
81.36.38.122	25851	172.16.0.122	80	1	54	0	0	1	54	26.415975	0.0000	—	—
77.125.22.149	1063	172.16.0.122	80	423	377 k	262	367 k	161	9296	26.578456	18.7531	156 k	3965
217.119.117.212	3603	172.16.0.122	80	9	1990	5	1123	4	867	31.647747	0.5684	15 k	12 k
41.232.66.192	60523	172.16.0.122	80	17	1967	9	952	8	1015	33.780133	1.5249	4994	5324
86.158.82.212	4962	172.16.0.122	80	9	1527	5	641	4	886	36.592159	15.3524	334	461
85.18.14.19	14399	172.16.0.122	80	26	11 k	10	6953	16	4129	43.211651	93.4882	594	353
217.119.117.212	3609	172.16.0.122	80	11	3046	6	2125	5	921	44.536196	0.6076	27 k	12 k
80.91.112.106	52995	172.16.0.122	80	10	2595	6	2315	4	280	45.468204	3.3352	5552	671
83.190.80.105	2300	172.16.0.122	80	9	1491	5	623	4	868	52.126180	15.4955	321	448
89.85.51.194	1099	172.16.0.122	80	12	2658	6	1737	6	921	54.758281	0.4205	33 k	17 k
80.90.81.206	2134	172.16.0.122	80	22	9989	11	8762	11	1227	57.683232	12.8947	5436	761
217.119.117.212	3629	172.16.0.122	80	11	2869	6	1936	5	933	58.483801	3.6900	4197	2022
41.250.23.6	45825	172.16.0.122	80	12	3162	7	2195	5	967	72.448185	12.1828	1441	634
217.119.117.212	3641	172.16.0.122	80	9	1926	5	1059	4	867	73.904674	0.6696	12 k	10 k
200.121.1.131	10594	172.16.0.122	80	515	385 k	261	371 k	254	14 k	93.841385	28.8779	102 k	3960
200.72.43.226	62317	172.16.0.122	80	546	429 k	273	409 k	273	20 k	99.866905	29.3974	111 k	5473

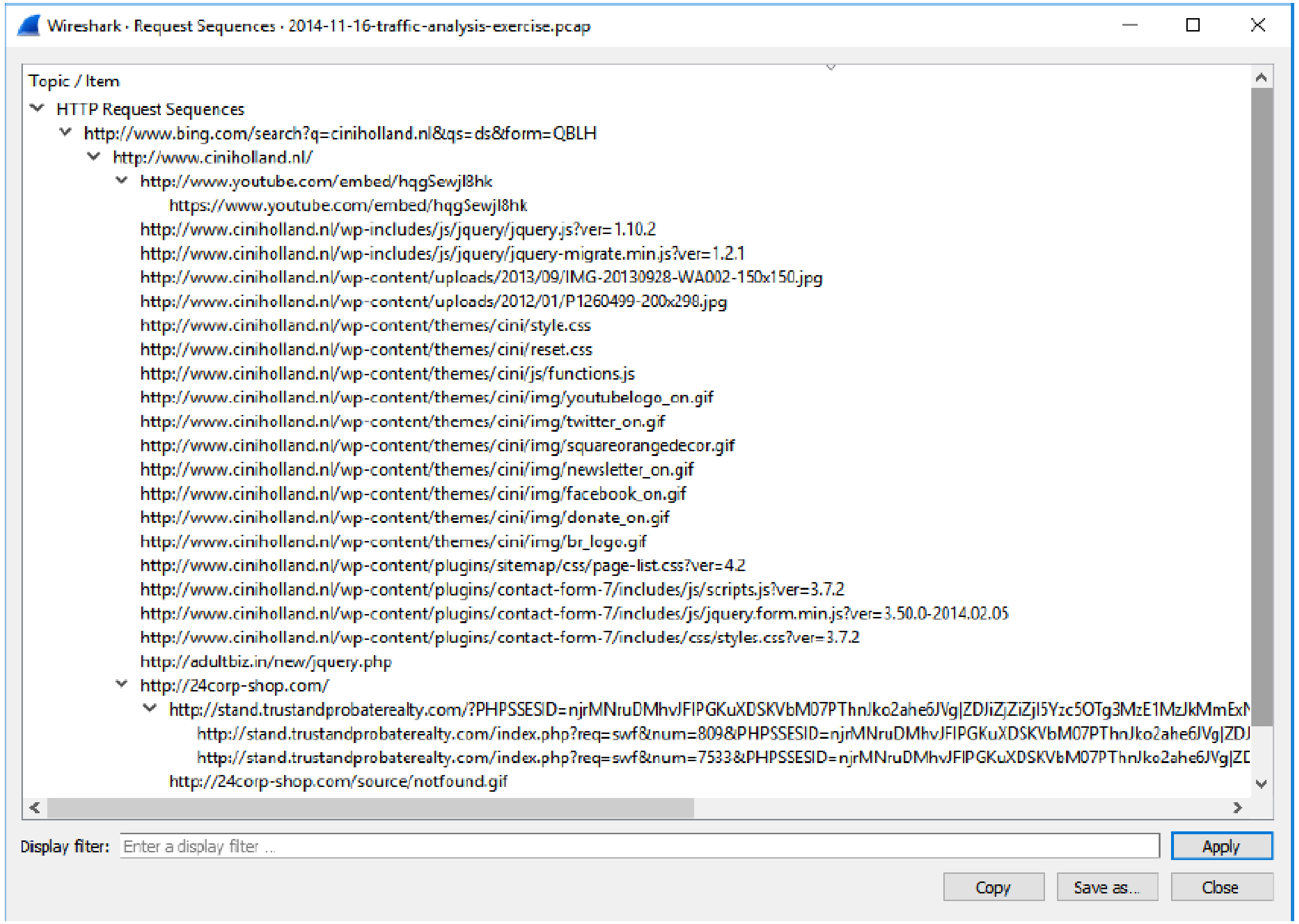
□ Name resolution □ Limit to display filter □ Absolute start time

Figure 75. The "Conversations" window

Source: Wireshark User's Guide

Review

Useful Wireshark Tips: Statistics



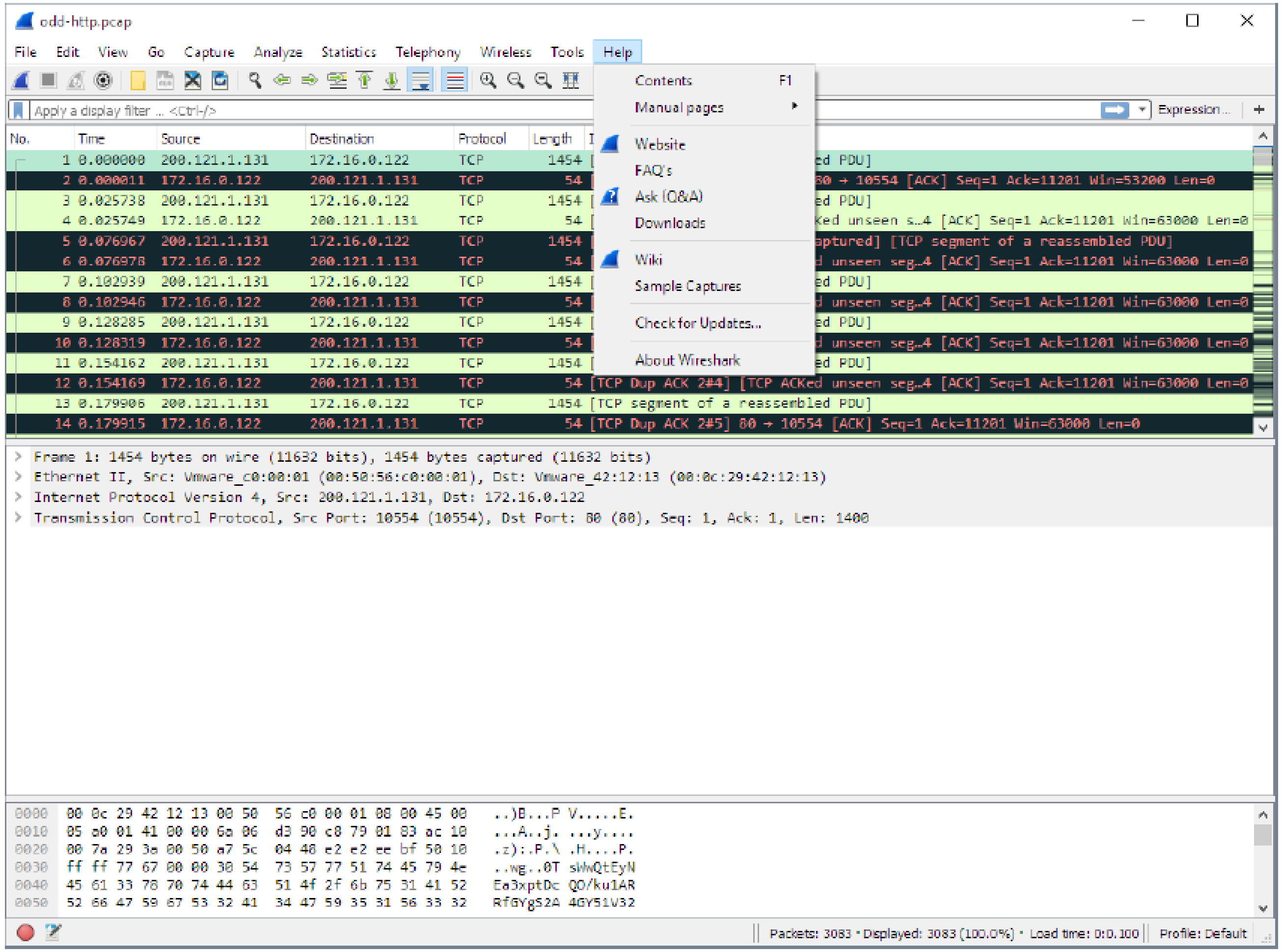
Wireshark · Request Sequences · 2014-11-16-traffic-analysis-exercise.pcap
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close

```
Topic / Item
HTTP Request Sequences
  http://www.bing.com/search?q=ciniholland.nl&qs=ds&form=QBLH
    http://www.ciniholland.nl/
      http://www.youtube.com/embed/hqgSewjl8hk
        https://www.youtube.com/embed/hqgSewjl8hk
      http://www.ciniholland.nl/wp-includes/js/jquery/jquery.js?ver=1.10.2
      http://www.ciniholland.nl/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1
      http://www.ciniholland.nl/wp-content/uploads/2013/09/IMG-20130928-WA002-150x150.jpg
      http://www.ciniholland.nl/wp-content/uploads/2012/01/P1260499-200x298.jpg
      http://www.ciniholland.nl/wp-content/themes/cini/style.css
      http://www.ciniholland.nl/wp-content/themes/cini/reset.css
      http://www.ciniholland.nl/wp-content/themes/cini/js/functions.js
      http://www.ciniholland.nl/wp-content/themes/cini/img/youtubelogo_on.gif
      http://www.ciniholland.nl/wp-content/themes/cini/img/twitter_on.gif
      http://www.ciniholland.nl/wp-content/themes/cini/img/squareorangedecor.gif
      http://www.ciniholland.nl/wp-content/themes/cini/img/newsletter_on.gif
      http://www.ciniholland.nl/wp-content/themes/cini/img/facebook_on.gif
      http://www.ciniholland.nl/wp-content/themes/cini/img/donate_on.gif
      http://www.ciniholland.nl/wp-content/themes/cini/img/br_logo.gif
      http://www.ciniholland.nl/wp-content/plugins/sitemap/css/page-list.css?ver=4.2
      http://www.ciniholland.nl/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=3.7.2
      http://www.ciniholland.nl/wp-content/plugins/contact-form-7/includes/js/jquery.form.min.js?ver=3.50.0-2014.02.05
      http://www.ciniholland.nl/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=3.7.2
      http://adultbiz.in/new/jquery.php
      http://24corp-shop.com/
        http://stand.trustandprobaterealty.com/?PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN
          http://stand.trustandprobaterealty.com/index.php?req=swf&num=809&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJ
          http://stand.trustandprobaterealty.com/index.php?req=swf&num=7533&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZD
        http://24corp-shop.com/source/notfound.gif
```

Figure 80. The "HTTP Request Sequences" window

Source: Wireshark User's Guide

Useful Wireshark Tips: Help



```
No.  Time       Source          Destination     Protocol  Length  I
   1 0.000000   200.121.1.131   172.16.0.122    TCP       1454 [                              ed PDU]
   2 0.000011   172.16.0.122    200.121.1.131   TCP         54 [                              80 → 10554 [ACK] Seq=1 Ack=11201 Win=53200 Len=0
   3 0.025738   200.121.1.131   172.16.0.122    TCP       1454 [                              ed PDU]
   4 0.025749   172.16.0.122    200.121.1.131   TCP         54 [                              Ked unseen s…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
   5 0.076967   200.121.1.131   172.16.0.122    TCP       1454 [                              aptured] [TCP segment of a reassembled PDU]
   6 0.076978   172.16.0.122    200.121.1.131   TCP         54 [                              d unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
   7 0.102939   200.121.1.131   172.16.0.122    TCP       1454 [                              ed PDU]
   8 0.102946   172.16.0.122    200.121.1.131   TCP         54 [                              d unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
   9 0.128285   200.121.1.131   172.16.0.122    TCP       1454 [                              ed PDU]
  10 0.128319   172.16.0.122    200.121.1.131   TCP         54 [                              d unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
  11 0.154162   200.121.1.131   172.16.0.122    TCP       1454 [                              ed PDU]
  12 0.154169   172.16.0.122    200.121.1.131   TCP         54 [TCP Dup ACK 2#4] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
  13 0.179906   200.121.1.131   172.16.0.122    TCP       1454 [TCP segment of a reassembled PDU]
  14 0.179915   172.16.0.122    200.121.1.131   TCP         54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
```

```
> Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
> Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
> Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
> Transmission Control Protocol, Src Port: 10554 (10554), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1400
```

```
0000  00 0c 29 42 12 13 00 50  56 c0 00 01 08 00 45 00   ..)B...P V.....E.
0010  05 a0 01 41 00 00 6a 06  d3 90 c8 79 01 83 ac 10   ...A..j. ...y....
0020  00 7a 29 3a 00 50 a7 5c  04 48 e2 e2 ee bf 50 10   .z):.P.\ .H....P.
0030  ff ff 77 67 00 00 30 54  73 57 77 51 74 45 79 4e   ..wg..0T sWwQtEyN
0040  45 61 33 78 70 74 44 63  51 4f 2f 6b 75 31 41 52   Ea3xptDc QO/ku1AR
0050  52 66 47 59 67 53 32 41  34 47 59 35 31 56 33 32   RfGYgS2A 4GY51V32
```

Packets: 3083 · Displayed: 3083 (100.0%) · Load time: 0:0.100 | Profile: Default

Source: Wireshark User's Guide

Network Traffic Analysis

- Another **possible way** of inspecting network traffic: by using a ***Network Forensics Analysis Tool (NFAT)***
- The tool can also **extract** the contained applications data from a captured Internet traffic
- Examples: **NetworkMiner** & **Xplico** *(discussed next)*

Network Forensics Analysis Tools (NetworkMiner & Xplico)

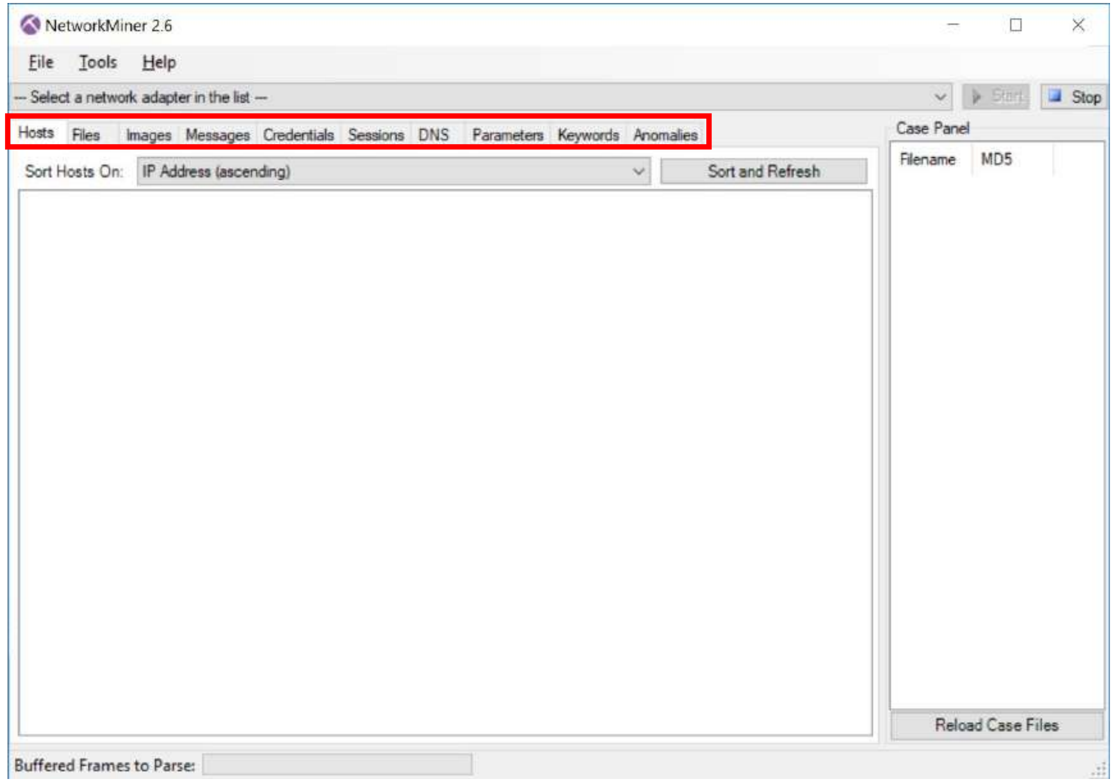
Network Traffic Analysis

- Another **possible way** of inspecting network traffic: by using a ***Network Forensics Analysis Tool (NFAT)***
- Examples: **NetMiner, Xplico**

- They can **extract** the contained ***applications data/objects*** from a captured Internet traffic
- Several **object types**
- **Very useful** network & Internet forensics tools!

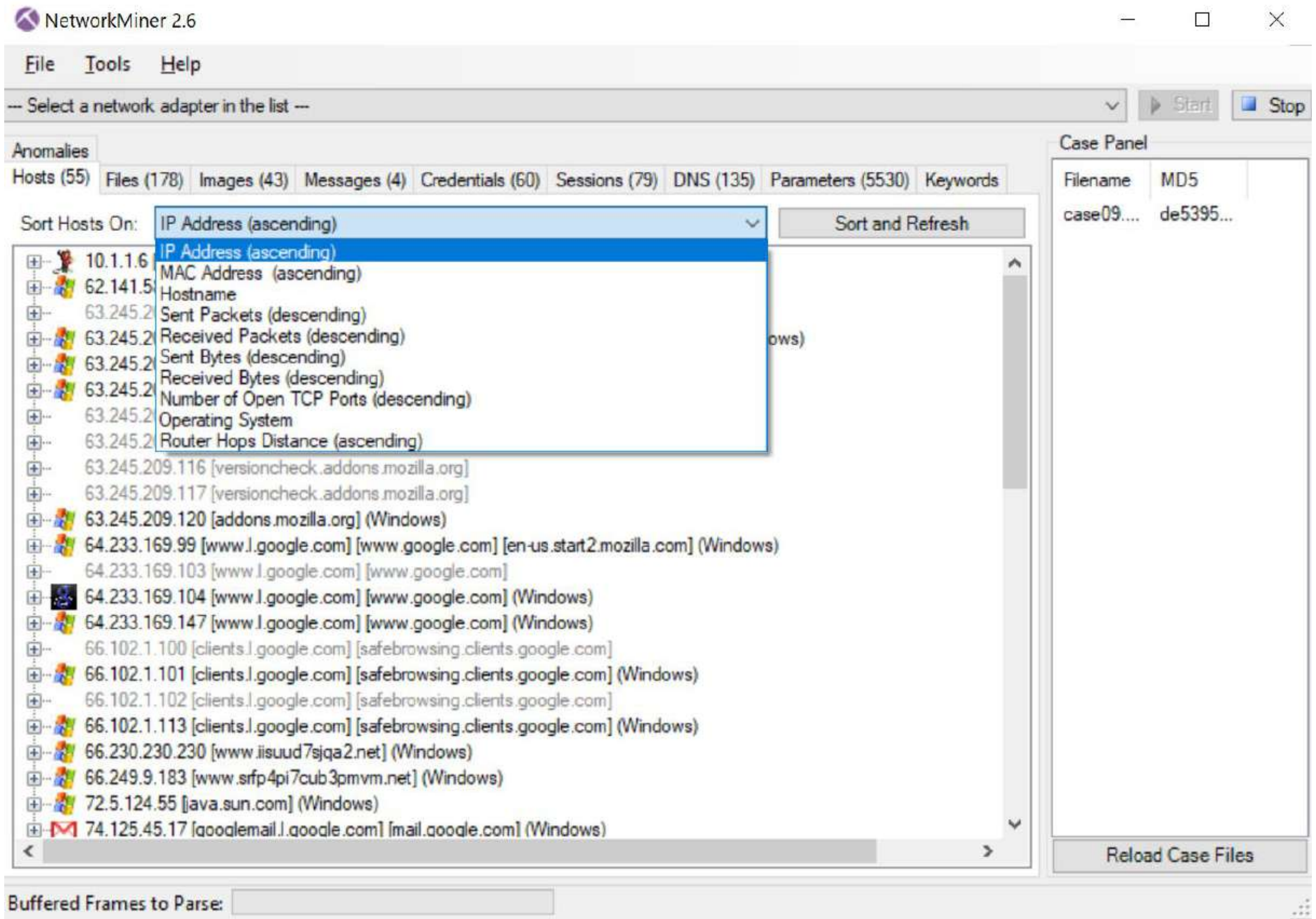
NetworkMiner

- An **open-source** NFAT for Windows (also works in Linux / Mac OS X / FreeBSD)
- Performs **life** sniffing or **PCAP analysis**
- Parses PCAP files for **offline** traffic analysis:
  - Focus on ***objects*** (hosts, transmitted contents, certificates) & ***their attributes*** rather than network packets
  - Corresponding several **tabs** in its GUI
- Versions: Free edition & Professional (see: https://www.netresec.com/?page=networkminer)
- Evident analysis using NetworkMiner: **Lab 7**



Sort Hosts On: IP Address (ascending)

NetworkMiner: Hosts



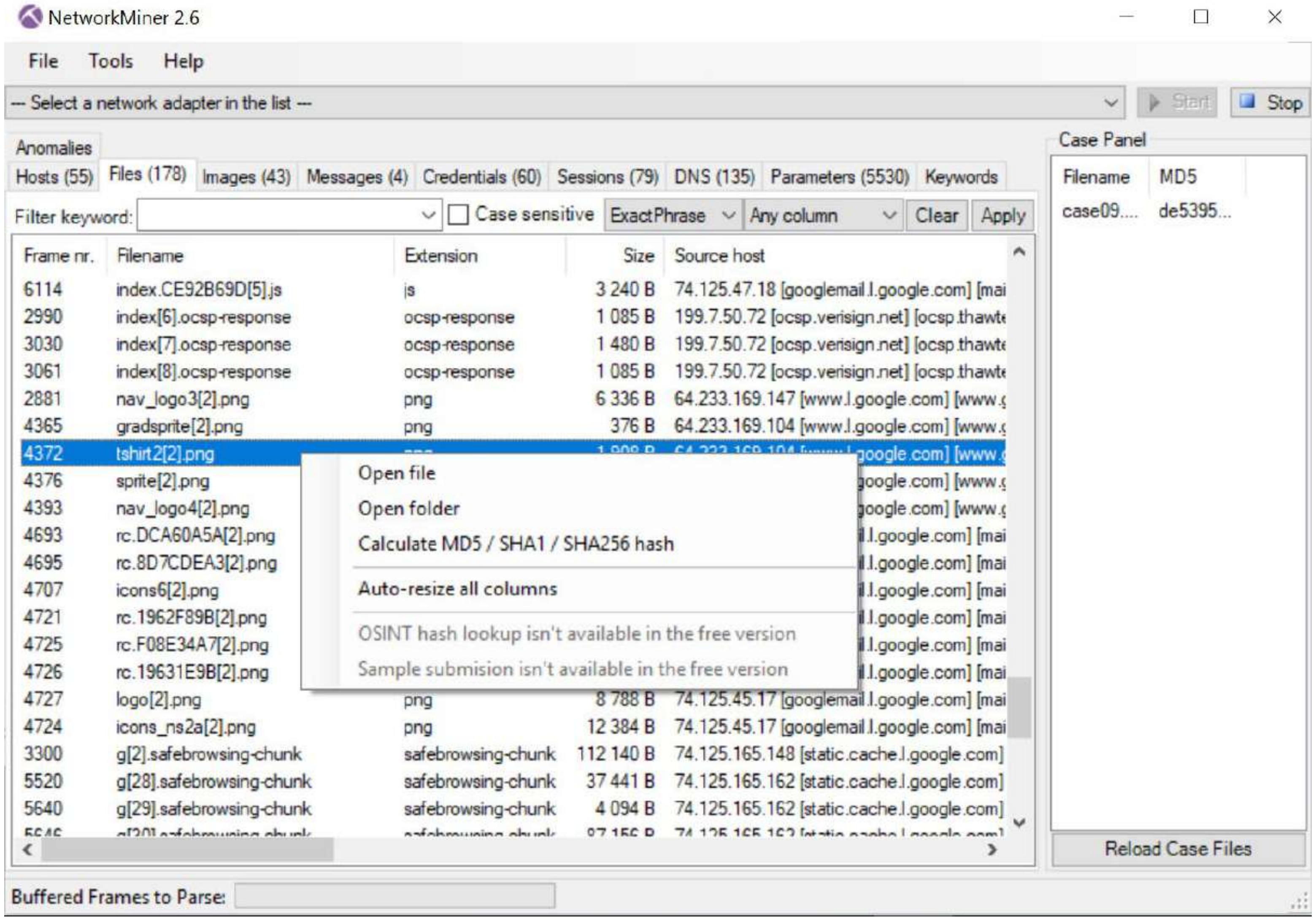
Filename	MD5
case09....	de5395...

```
10.1.1.6
62.141.5
63.245.2
63.245.2                                                              ows)
63.245.2
63.245.2
63.245.2
63.245.2
63.245.209.116 [versioncheck.addons.mozilla.org]
63.245.209.117 [versioncheck.addons.mozilla.org]
63.245.209.120 [addons.mozilla.org] (Windows)
64.233.169.99 [www.l.google.com] [www.google.com] [en-us.start2.mozilla.com] (Windows)
64.233.169.103 [www.l.google.com] [www.google.com]
64.233.169.104 [www.l.google.com] [www.google.com] (Windows)
64.233.169.147 [www.l.google.com] [www.google.com] (Windows)
66.102.1.100 [clients.l.google.com] [safebrowsing.clients.google.com]
66.102.1.101 [clients.l.google.com] [safebrowsing.clients.google.com] (Windows)
66.102.1.102 [clients.l.google.com] [safebrowsing.clients.google.com]
66.102.1.113 [clients.l.google.com] [safebrowsing.clients.google.com] (Windows)
66.230.230.230 [www.iisuud7sjqa2.net] (Windows)
66.249.9.183 [www.srfp4pi7cub3pmvm.net] (Windows)
72.5.124.55 [java.sun.com] (Windows)
74.125.45.17 [googlemail.l.google.com] [mail.google.com] (Windows)
```

NetworkMiner: Hosts

- Lists all **hosts** found in the analyzed network traffic by:
  - IP address
  - MAC address
  - Hostname
  - Sent & received packet
  - Port number
  - OS
- **Additional properties** about hosts are also shown

NetworkMiner: Files



Frame nr.	Filename	Extension	Size	Source host
6114	index.CE92B69D[5].js	js	3 240 B	74.125.47.18 [googlemail.l.google.com] [mai
2990	index[6].ocsp-response	ocsp-response	1 085 B	199.7.50.72 [ocsp.verisign.net] [ocsp.thawte
3030	index[7].ocsp-response	ocsp-response	1 480 B	199.7.50.72 [ocsp.verisign.net] [ocsp.thawte
3061	index[8].ocsp-response	ocsp-response	1 085 B	199.7.50.72 [ocsp.verisign.net] [ocsp.thawte
2881	nav_logo3[2].png	png	6 336 B	64.233.169.147 [www.l.google.com] [www.g
4365	gradsprite[2].png	png	376 B	64.233.169.104 [www.l.google.com] [www.g
4372	tshirt2[2].png	png	1 908 B	64.233.169.104 [www.l.google.com] [www.g
4376	sprite[2].png			google.com] [www.g
4393	nav_logo4[2].png			google.com] [www.g
4693	rc.DCA60A5A[2].png			l.google.com] [mai
4695	rc.8D7CDEA3[2].png			l.google.com] [mai
4707	icons6[2].png			l.google.com] [mai
4721	rc.1962F89B[2].png			l.google.com] [mai
4725	rc.F08E34A7[2].png			l.google.com] [mai
4726	rc.19631E9B[2].png			l.google.com] [mai
4727	logo[2].png	png	8 788 B	74.125.45.17 [googlemail.l.google.com] [mai
4724	icons_ns2a[2].png	png	12 384 B	74.125.45.17 [googlemail.l.google.com] [mai
3300	g[2].safebrowsing-chunk	safebrowsing-chunk	112 140 B	74.125.165.148 [static.cache.l.google.com]
5520	g[28].safebrowsing-chunk	safebrowsing-chunk	37 441 B	74.125.165.162 [static.cache.l.google.com]
5640	g[29].safebrowsing-chunk	safebrowsing-chunk	4 094 B	74.125.165.162 [static.cache.l.google.com]

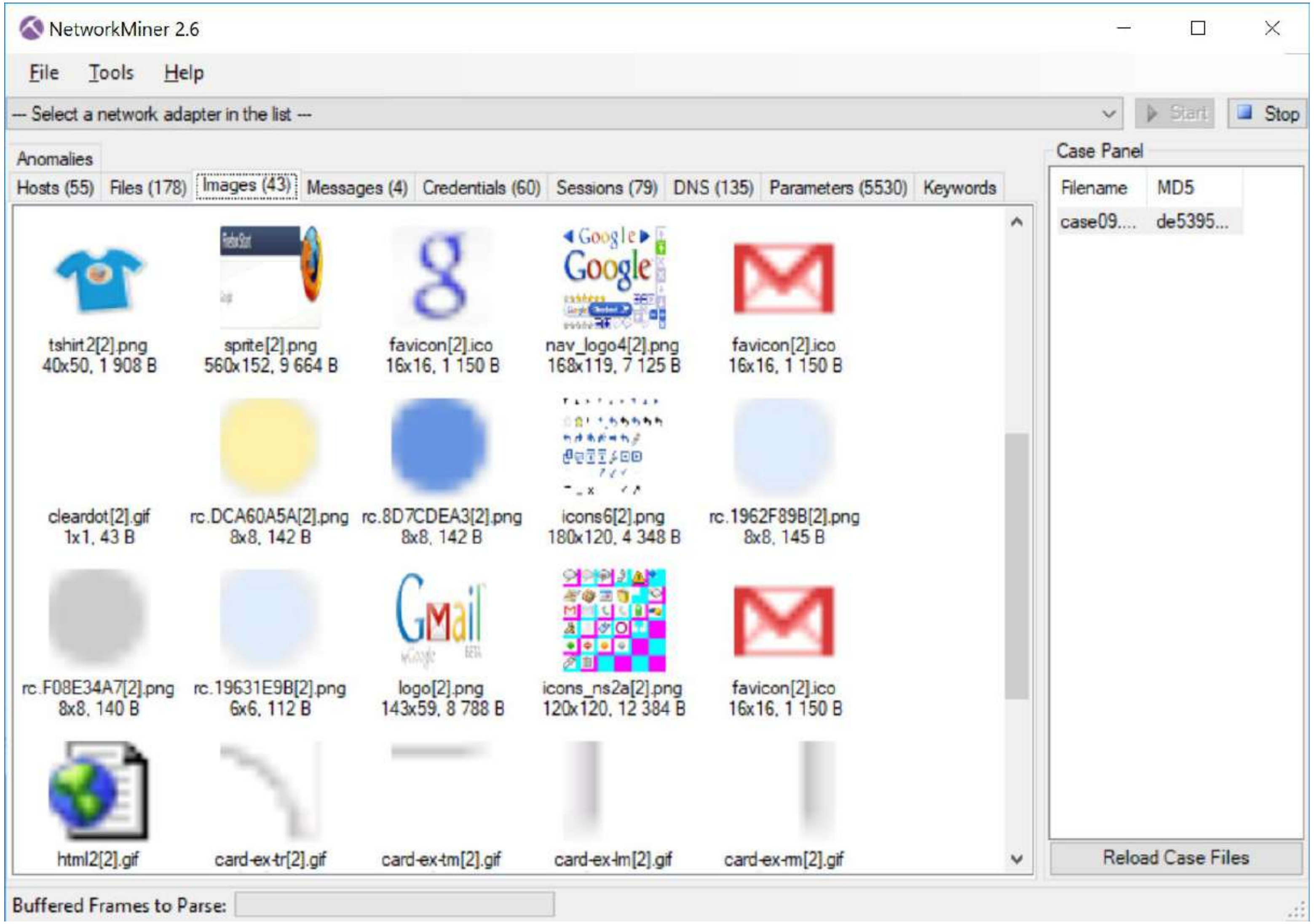
Case Panel

Filename	MD5
case09....	de5395...

NetworkMiner: Files

- Lists all **files** that have been reassembled and extracted by NetworkMiner
- Some ***file attributes*** shown include:
    - Filename
    - Extension
    - Source
    - Destination
    - Protocol
    - Port numbers
- Right-click a listed file to **open** it (*be careful with potentially malicious executables!*), calculate its hash values

NetworkMiner: Images



NetworkMiner 2.6

Filename	MD5
case09....	de5395...

tshirt2[2].png 40x50, 1 908 B

sprite[2].png 560x152, 9 664 B

favicon[2].ico 16x16, 1 150 B

nav_logo4[2].png 168x119, 7 125 B

favicon[2].ico 16x16, 1 150 B

cleardot[2].gif 1x1, 43 B

rc.DCA60A5A[2].png 8x8, 142 B

rc.8D7CDEA3[2].png 8x8, 142 B

icons6[2].png 180x120, 4 348 B

rc.1962F89B[2].png 8x8, 145 B

rc.F08E34A7[2].png 8x8, 140 B

rc.19631E9B[2].png 6x6, 112 B

logo[2].png 143x59, 8 788 B

icons_ns2a[2].png 120x120, 12 384 B

favicon[2].ico 16x16, 1 150 B

html2[2].gif

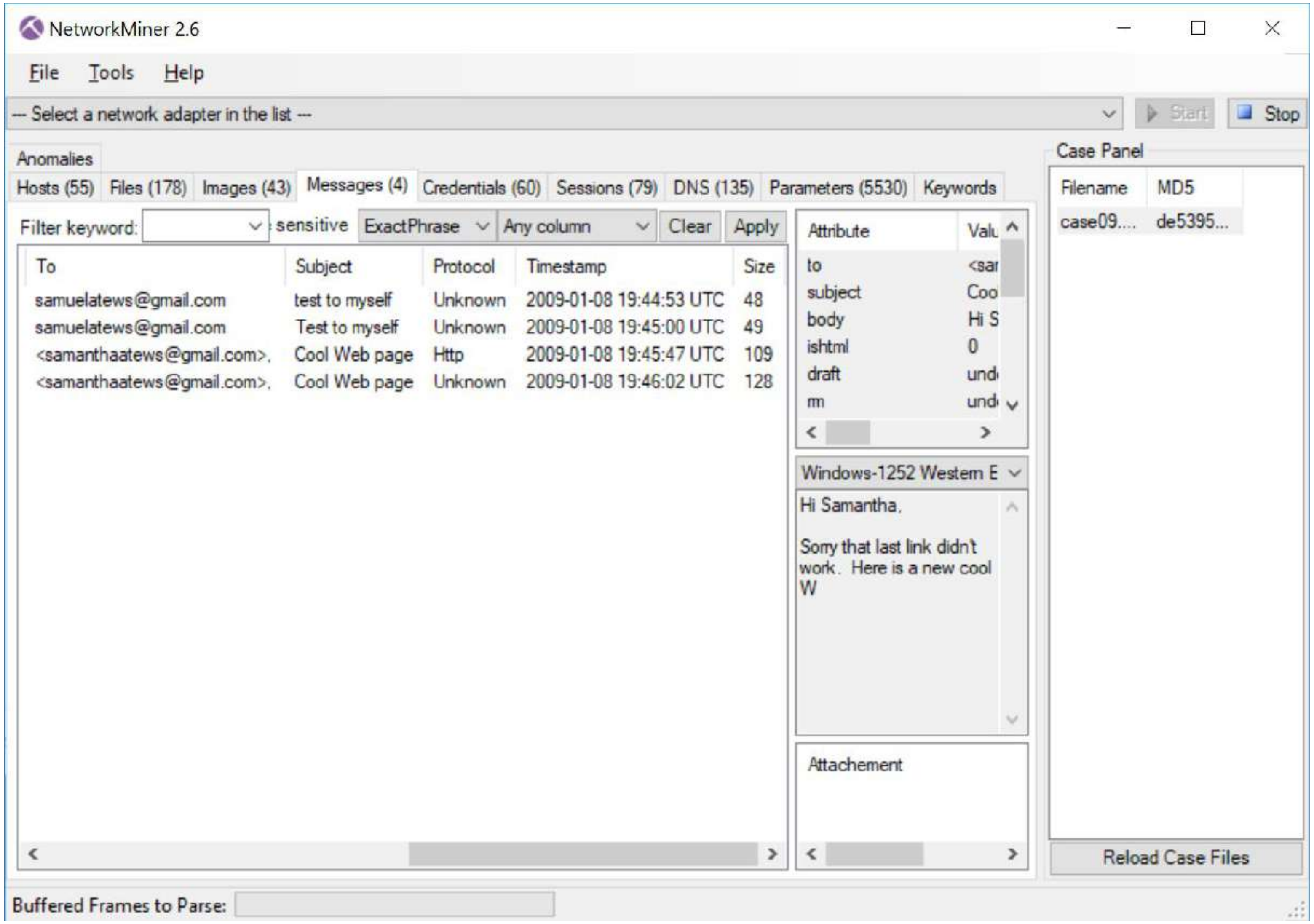
card-ex-tr[2].gif

card-ex-tm[2].gif

card-ex-lm[2].gif

card-ex-rm[2].gif

NetworkMiner: Messages



To	Subject	Protocol	Timestamp	Size
samuelatews@gmail.com	test to myself	Unknown	2009-01-08 19:44:53 UTC	48
samuelatews@gmail.com	Test to myself	Unknown	2009-01-08 19:45:00 UTC	49
<samanthaatews@gmail.com>,	Cool Web page	Http	2009-01-08 19:45:47 UTC	109
<samanthaatews@gmail.com>,	Cool Web page	Unknown	2009-01-08 19:46:02 UTC	128

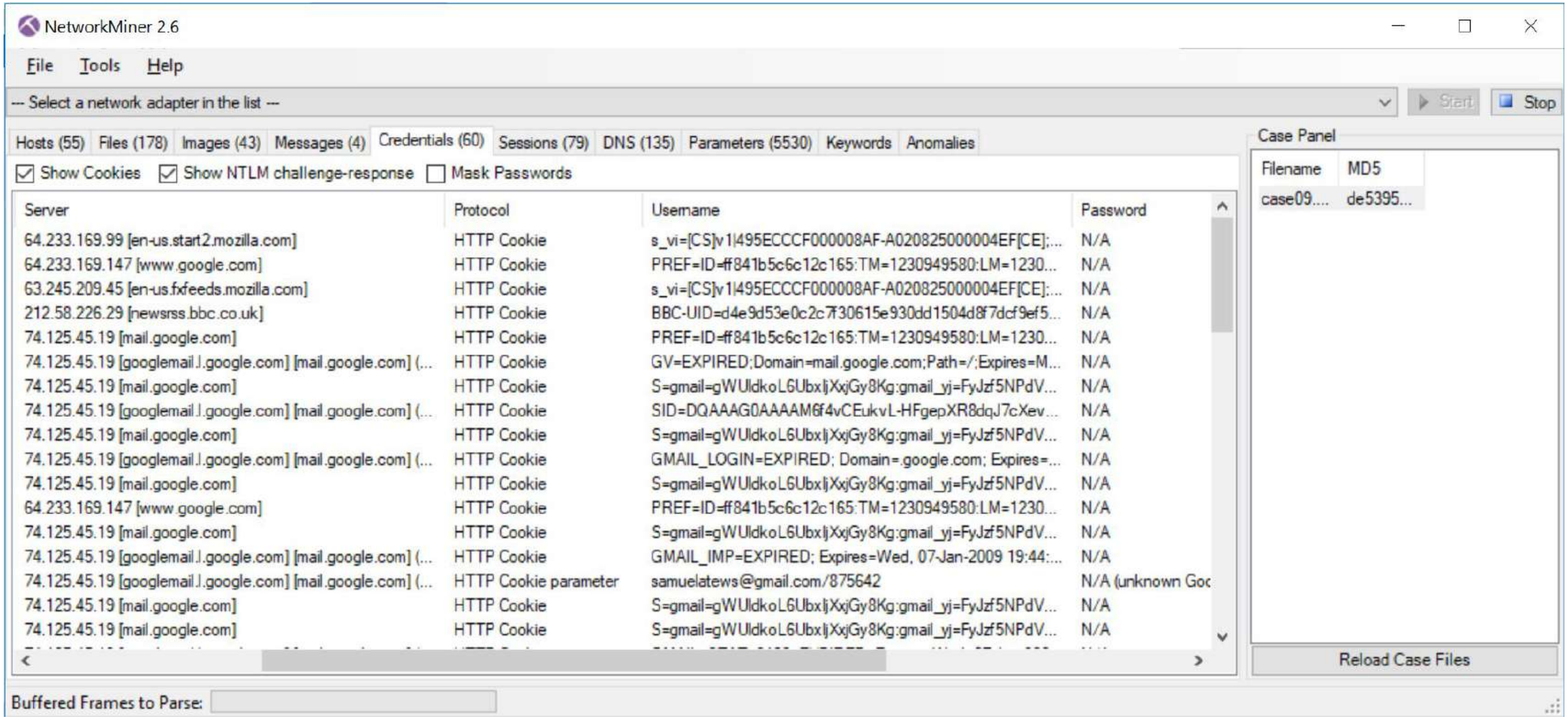
Attribute	Valu
to	<sar
subject	Coo
body	Hi S
ishtml	0
draft	und
rm	und

Hi Samantha,

Sorry that last link didn't work. Here is a new cool W

Filename	MD5
case09....	de5395...

NetworkMiner: Credentials

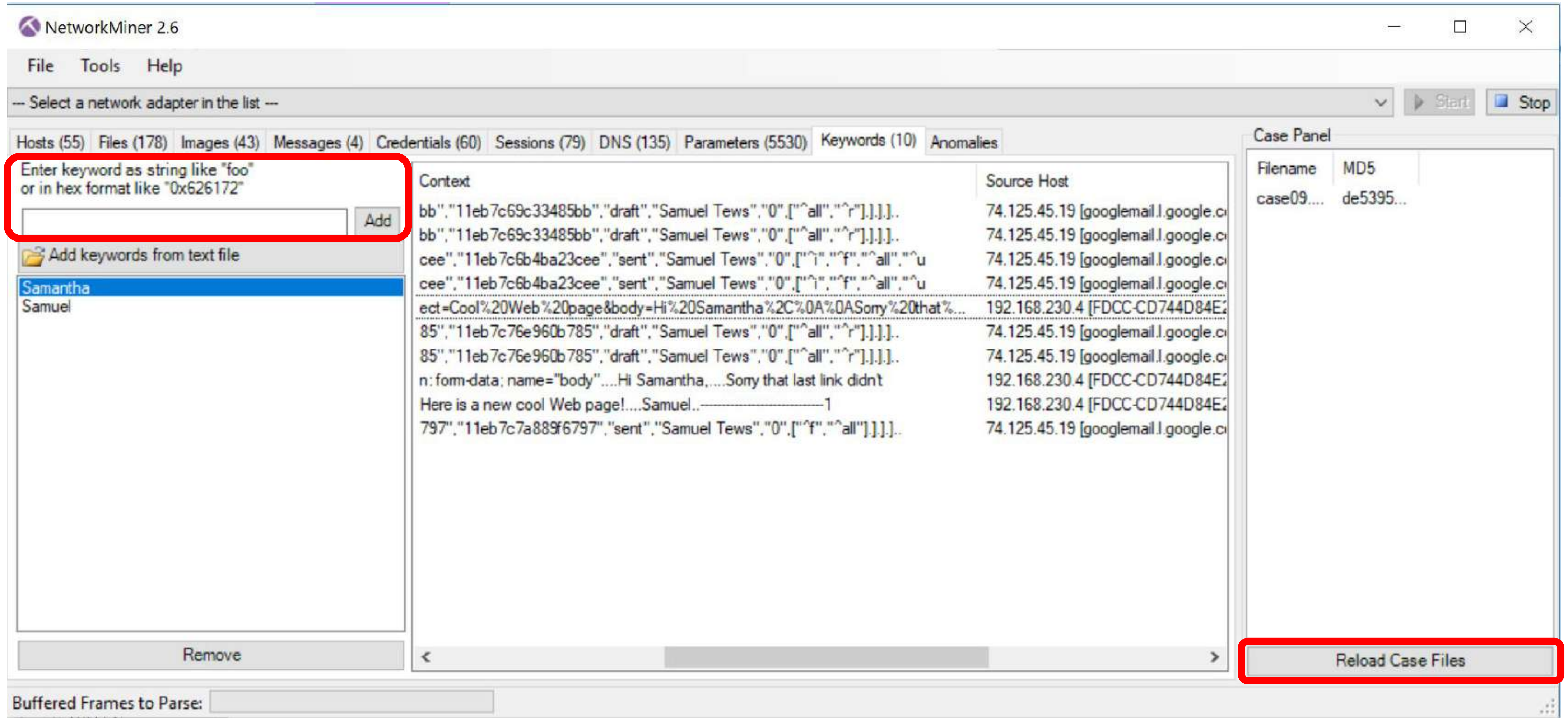


☑ Show Cookies ☑ Show NTLM challenge-response □ Mask Passwords

Server	Protocol	Username	Password
64.233.169.99 [en-us.start2.mozilla.com]	HTTP Cookie	s_vi=[CS]v1|495ECCCF000008AF-A020825000004EF[CE];...	N/A
64.233.169.147 [www.google.com]	HTTP Cookie	PREF=ID=ff841b5c6c12c165:TM=1230949580:LM=1230...	N/A
63.245.209.45 [en-us.fxfeeds.mozilla.com]	HTTP Cookie	s_vi=[CS]v1|495ECCCF000008AF-A020825000004EF[CE];...	N/A
212.58.226.29 [newsrss.bbc.co.uk]	HTTP Cookie	BBC-UID=d4e9d53e0c2c7f30615e930dd1504d8f7dcf9ef5...	N/A
74.125.45.19 [mail.google.com]	HTTP Cookie	PREF=ID=ff841b5c6c12c165:TM=1230949580:LM=1230...	N/A
74.125.45.19 [googlemail.l.google.com] [mail.google.com] (...	HTTP Cookie	GV=EXPIRED;Domain=mail.google.com;Path=/;Expires=M...	N/A
74.125.45.19 [mail.google.com]	HTTP Cookie	S=gmail=gWUldkoL6UbxljXxjGy8Kg:gmail_yj=FyJzf5NPdV...	N/A
74.125.45.19 [googlemail.l.google.com] [mail.google.com] (...	HTTP Cookie	SID=DQAAAG0AAAAM6f4vCEukvL-HFgepXR8dqJ7cXev...	N/A
74.125.45.19 [mail.google.com]	HTTP Cookie	S=gmail=gWUldkoL6UbxljXxjGy8Kg:gmail_yj=FyJzf5NPdV...	N/A
74.125.45.19 [googlemail.l.google.com] [mail.google.com] (...	HTTP Cookie	GMAIL_LOGIN=EXPIRED; Domain=.google.com; Expires=...	N/A
74.125.45.19 [mail.google.com]	HTTP Cookie	S=gmail=gWUldkoL6UbxljXxjGy8Kg:gmail_yj=FyJzf5NPdV...	N/A
64.233.169.147 [www.google.com]	HTTP Cookie	PREF=ID=ff841b5c6c12c165:TM=1230949580:LM=1230...	N/A
74.125.45.19 [mail.google.com]	HTTP Cookie	S=gmail=gWUldkoL6UbxljXxjGy8Kg:gmail_yj=FyJzf5NPdV...	N/A
74.125.45.19 [googlemail.l.google.com] [mail.google.com] (...	HTTP Cookie	GMAIL_IMP=EXPIRED; Expires=Wed, 07-Jan-2009 19:44:...	N/A
74.125.45.19 [googlemail.l.google.com] [mail.google.com] (...	HTTP Cookie parameter	samuelatews@gmail.com/875642	N/A (unknown Goc
74.125.45.19 [mail.google.com]	HTTP Cookie	S=gmail=gWUldkoL6UbxljXxjGy8Kg:gmail_yj=FyJzf5NPdV...	N/A
74.125.45.19 [mail.google.com]	HTTP Cookie	S=gmail=gWUldkoL6UbxljXxjGy8Kg:gmail_yj=FyJzf5NPdV...	N/A

Filename	MD5
case09....	de5395...

NetworkMiner: Keywords



Enter keyword as string like "foo"
or in hex format like "0x626172"

Samantha
Samuel

Context	Source Host
bb","11eb7c69c33485bb","draft","Samuel Tews","0",["^all","^r"]]]]..	74.125.45.19 [googlemail.l.google.c
bb","11eb7c69c33485bb","draft","Samuel Tews","0",["^all","^r"]]]]..	74.125.45.19 [googlemail.l.google.c
cee","11eb7c6b4ba23cee","sent","Samuel Tews","0",["^i","^f","^all","^u	74.125.45.19 [googlemail.l.google.c
cee","11eb7c6b4ba23cee","sent","Samuel Tews","0",["^i","^f","^all","^u	74.125.45.19 [googlemail.l.google.c
ect=Cool%20Web%20page&body=Hi%20Samantha%2C%0A%0ASorry%20that%...	192.168.230.4 [FDCC-CD744D84E
85","11eb7c76e960b785","draft","Samuel Tews","0",["^all","^r"]]]]..	74.125.45.19 [googlemail.l.google.c
85","11eb7c76e960b785","draft","Samuel Tews","0",["^all","^r"]]]]..	74.125.45.19 [googlemail.l.google.c
n: form-data; name="body"....Hi Samantha,....Sorry that last link didn't	192.168.230.4 [FDCC-CD744D84E
Here is a new cool Web page!....Samuel..-----------------------1	192.168.230.4 [FDCC-CD744D84E
797","11eb7c7a889f6797","sent","Samuel Tews","0",["^f","^all"]]]]..	74.125.45.19 [googlemail.l.google.c

Filename	MD5
case09....	de5395...

NetworkMiner: References

- Some **resources**:
  - Download site: https://www.netresec.com/?page=networkminer
  - **Videos**:
    - "*NetworkMiner Video Tutorials on the Intertubes*": https://www.netresec.com/?page=Blog&month=2011-02&post=NetworkMiner-Video-Tutorials-on-the-Intertubes
    - "*Zyklon Malware Network Forensics Video Tutorial*": https://www.netresec.com/?page=Blog&month=2018-02&post=Zyklon-Malware-Network-Forensics-Video-Tutorial,
  - Sample usage on a **PCAP file**: https://www.netresec.com/?page=Blog&month=2011-01&post=Analyzing-the-TCPIP-Weapons-School-Sample-Lab

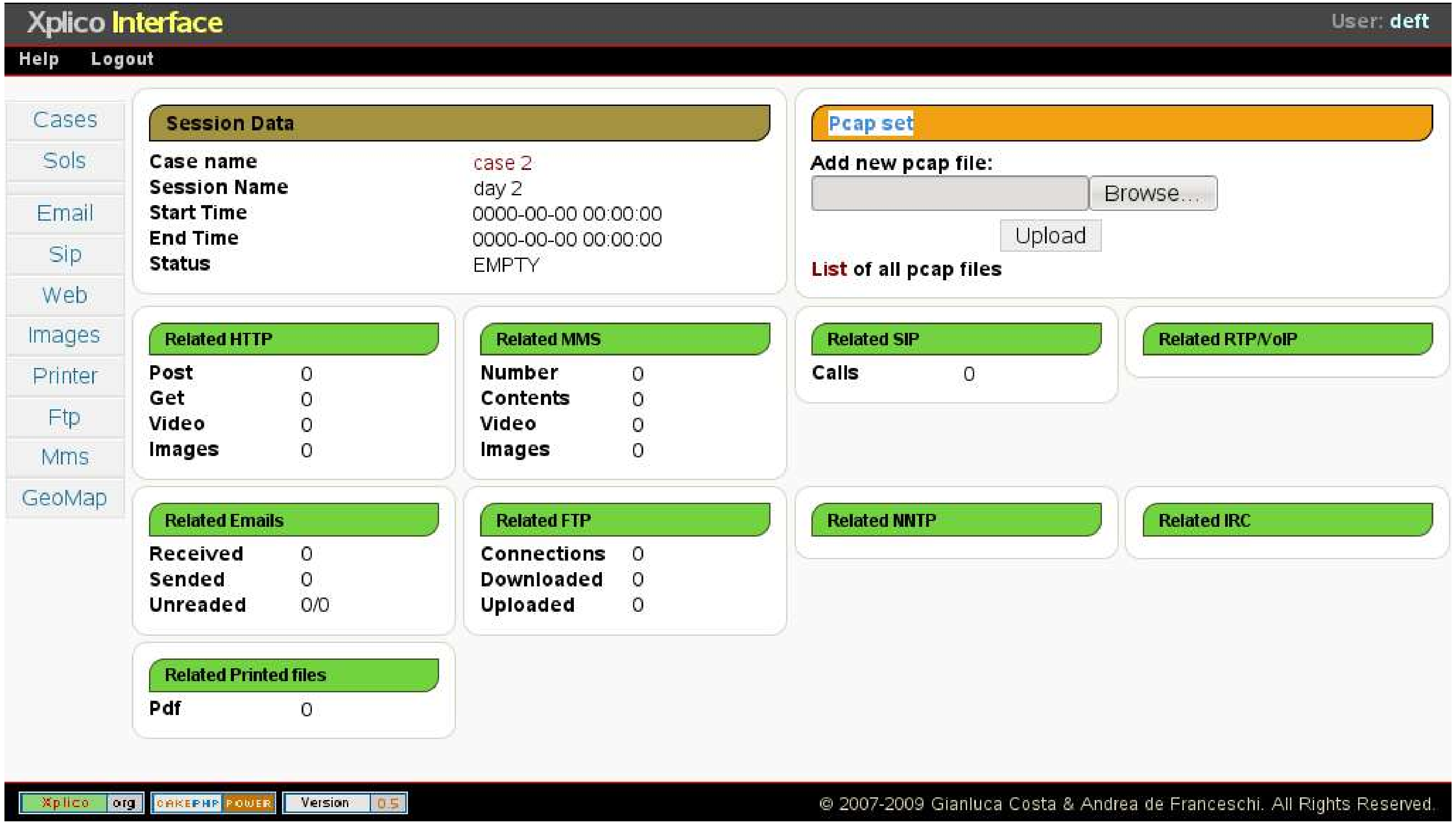
Xplico

- An **open source** Network Forensic Analysis Tool: released under the GNU GPL
- **Goal**: to extract the **contained applications data** from a captured Internet traffic
- **Use cases**: extract ***relevant evident*** from a pcap file, such as: emails (POP, IMAP, SMTP), HTTP contents, VoIP call (SIP), FTP, TFTP, etc.
- Note: Xplico ***is not*** a network packet/protocol analyzer

Xplico

- Some **features**:
  - Output data & information in **SQLite/Mysql database** and/or **files**
  - At each data reassembled by Xplico is associated an **XML file**: uniquely identifies the **flows** & the **pcap** containing the data reassembled
  - **Modularity**: each Xplico component (input interface, protocol decoder/dissector, output interface/dispatcher) is modular
- Evident analysis using Xplico: **Lab 7**

Xplico: Sample Analysis



Session Data

Case name	case 2
Session Name	day 2
Start Time	0000-00-00 00:00:00
End Time	0000-00-00 00:00:00
Status	EMPTY

Add new pcap file:

List of all pcap files

Related HTTP	
Post	0
Get	0
Video	0
Images	0

Related MMS	
Number	0
Contents	0
Video	0
Images	0

Related SIP	
Calls	0

Related RTP/VoIP

Related Emails	
Received	0
Sended	0
Unreaded	0/0

Related FTP	
Connections	0
Downloaded	0
Uploaded	0

Related NNTP

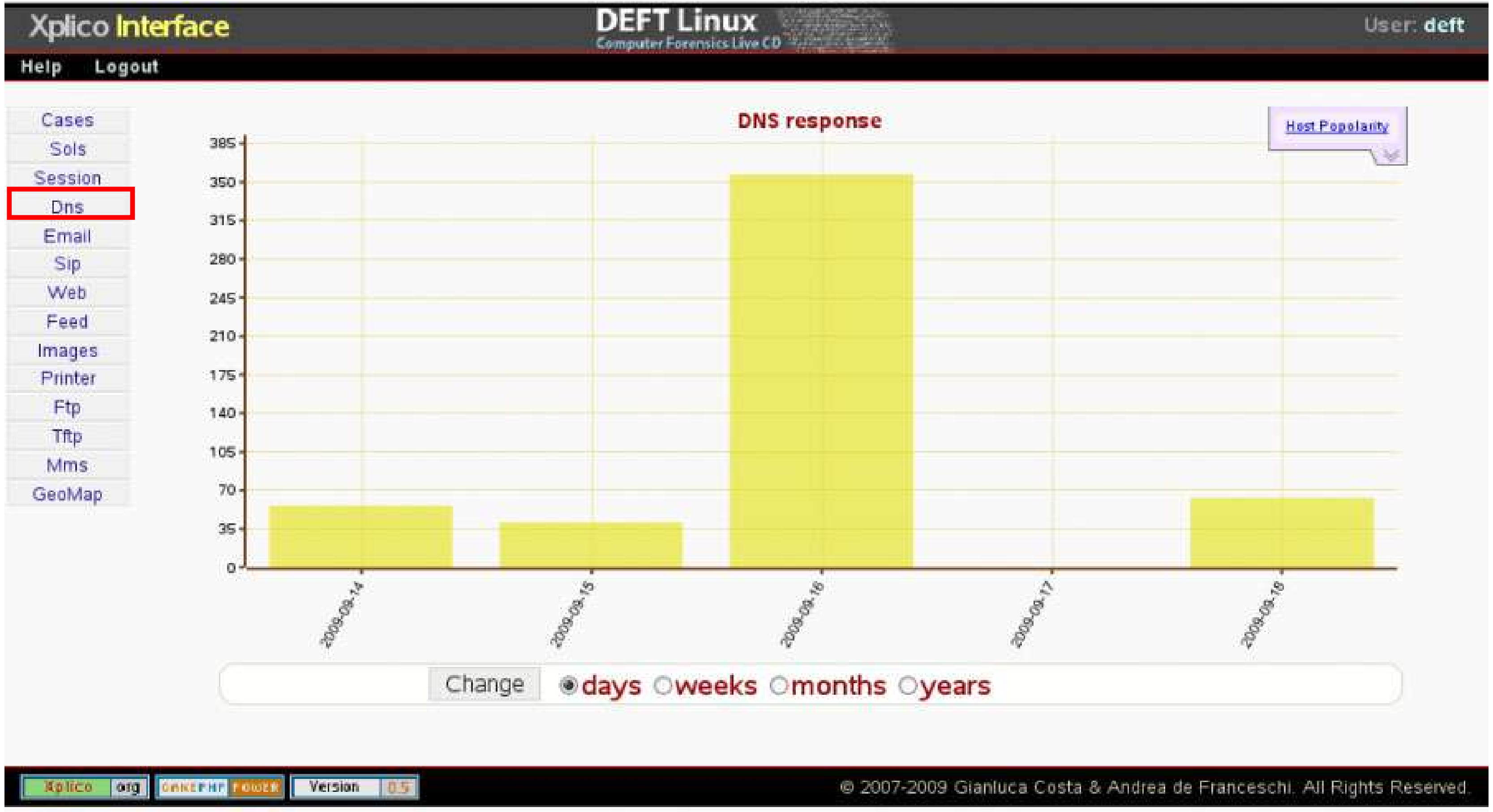
Related IRC

Related Printed files	
Pdf	0

© 2007-2009 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

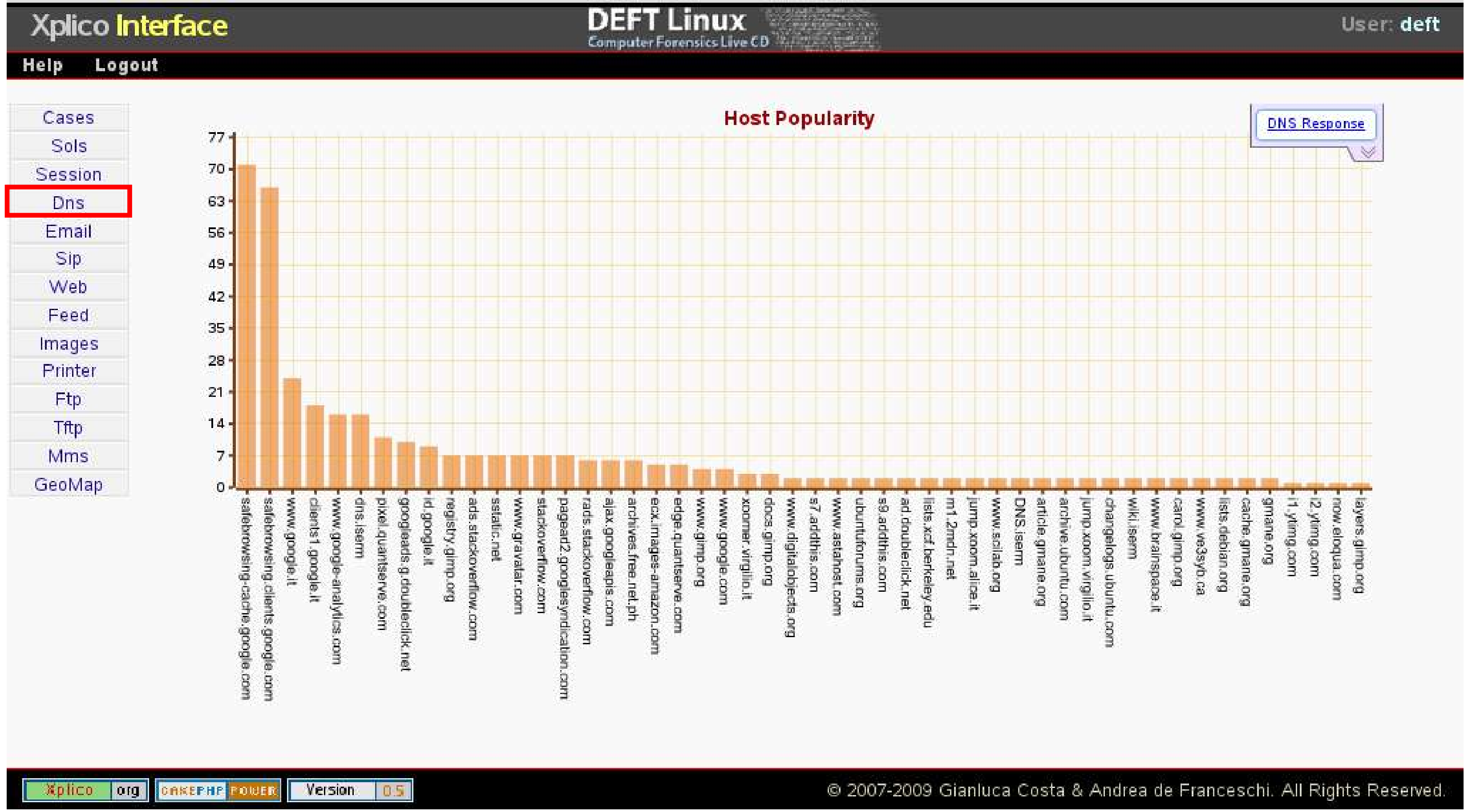
Source: https://www.xplico.org/screenshot

Xplico: Sample DNS Analysis



Source: https://www.xplico.org/screenshot

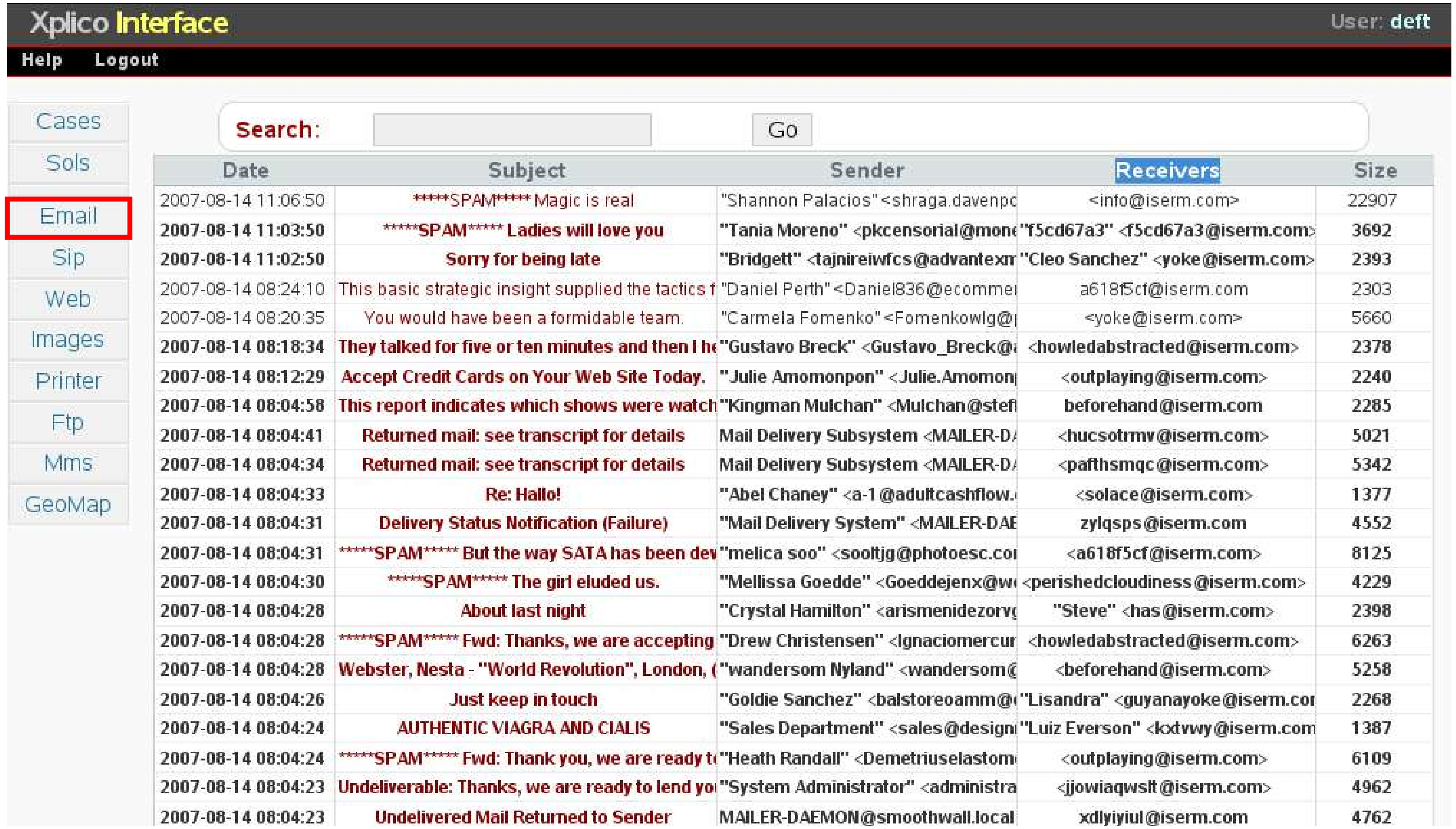
Xplico: Sample DNS Analysis



© 2007-2009 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

Source: https://www.xplico.org/screenshot

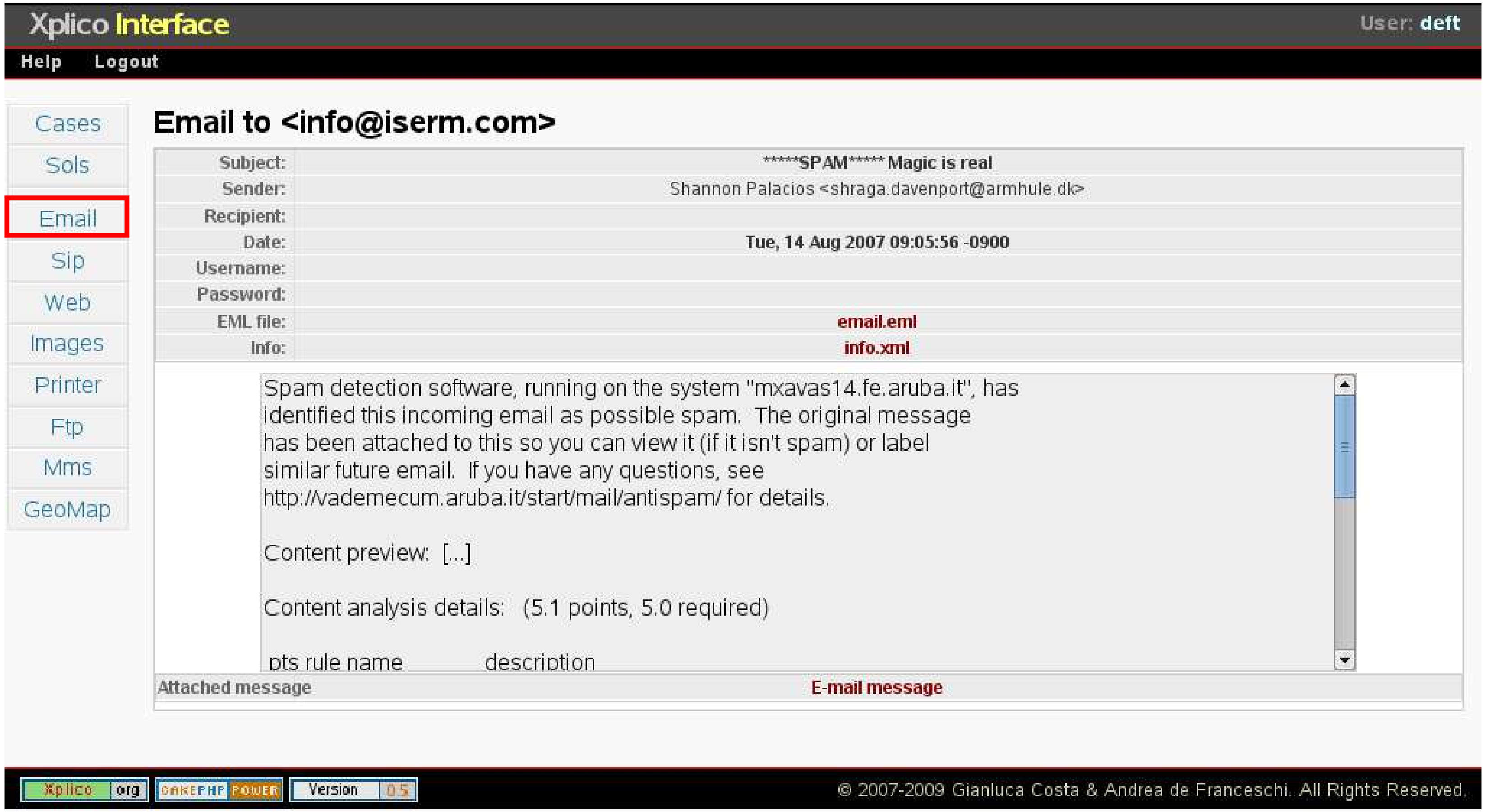
Xplico: Sample Email Analysis



Date	Subject	Sender	Receivers	Size
2007-08-14 11:06:50	*****SPAM***** Magic is real	"Shannon Palacios" <shraga.davenpc	<info@iserm.com>	22907
2007-08-14 11:03:50	*****SPAM***** Ladies will love you	"Tania Moreno" <pkcensorial@mone	"f5cd67a3" <f5cd67a3@iserm.com>	3692
2007-08-14 11:02:50	Sorry for being late	"Bridgett" <tajnireiwfcs@advantexm	"Cleo Sanchez" <yoke@iserm.com>	2393
2007-08-14 08:24:10	This basic strategic insight supplied the tactics f	"Daniel Perth" <Daniel836@ecommer	a618f5cf@iserm.com	2303
2007-08-14 08:20:35	You would have been a formidable team.	"Carmela Fomenko" <Fomenkowlg@	<yoke@iserm.com>	5660
2007-08-14 08:18:34	They talked for five or ten minutes and then I he	"Gustavo Breck" <Gustavo_Breck@	<howledabstracted@iserm.com>	2378
2007-08-14 08:12:29	Accept Credit Cards on Your Web Site Today.	"Julie Amomonpon" <Julie.Amomon	<outplaying@iserm.com>	2240
2007-08-14 08:04:58	This report indicates which shows were watch	"Kingman Mulchan" <Mulchan@stef	beforehand@iserm.com	2285
2007-08-14 08:04:41	Returned mail: see transcript for details	Mail Delivery Subsystem <MAILER-D	<hucsotrmv@iserm.com>	5021
2007-08-14 08:04:34	Returned mail: see transcript for details	Mail Delivery Subsystem <MAILER-D	<pafthsmqc@iserm.com>	5342
2007-08-14 08:04:33	Re: Hallo!	"Abel Chaney" <a-1@adultcashflow.	<solace@iserm.com>	1377
2007-08-14 08:04:31	Delivery Status Notification (Failure)	"Mail Delivery System" <MAILER-DAE	zylqsps@iserm.com	4552
2007-08-14 08:04:31	*****SPAM***** But the way SATA has been dev	"melica soo" <sooltjg@photoesc.co	<a618f5cf@iserm.com>	8125
2007-08-14 08:04:30	*****SPAM***** The girl eluded us.	"Mellissa Goedde" <Goeddejenx@w	<perishedcloudiness@iserm.com>	4229
2007-08-14 08:04:28	About last night	"Crystal Hamilton" <arismenidezorv	"Steve" <has@iserm.com>	2398
2007-08-14 08:04:28	*****SPAM***** Fwd: Thanks, we are accepting	"Drew Christensen" <Ignaciomercur	<howledabstracted@iserm.com>	6263
2007-08-14 08:04:28	Webster, Nesta - "World Revolution", London, (	"wandersom Nyland" <wandersom@	<beforehand@iserm.com>	5258
2007-08-14 08:04:26	Just keep in touch	"Goldie Sanchez" <balstoreoamm@	"Lisandra" <guyanayoke@iserm.co	2268
2007-08-14 08:04:24	AUTHENTIC VIAGRA AND CIALIS	"Sales Department" <sales@design	"Luiz Everson" <kxtvwy@iserm.com	1387
2007-08-14 08:04:24	*****SPAM***** Fwd: Thank you, we are ready t	"Heath Randall" <Demetriuselastom	<outplaying@iserm.com>	6109
2007-08-14 08:04:23	Undeliverable: Thanks, we are ready to lend yo	"System Administrator" <administra	<jjowiaqwslt@iserm.com>	4962
2007-08-14 08:04:23	Undelivered Mail Returned to Sender	MAILER-DAEMON@smoothwall.local	xdlyiyiul@iserm.com	4762

Source: https://www.xplico.org/screenshot

Xplico: Sample Email Analysis



Email to <info@iserm.com>

Subject:	*****SPAM***** Magic is real
Sender:	Shannon Palacios <shraga.davenport@armhule.dk>
Recipient:	
Date:	Tue, 14 Aug 2007 09:05:56 -0900
Username:	
Password:	
EML file:	email.eml
Info:	info.xml

Spam detection software, running on the system "mxavas14.fe.aruba.it", has
identified this incoming email as possible spam. The original message
has been attached to this so you can view it (if it isn't spam) or label
similar future email. If you have any questions, see
http://vademecum.aruba.it/start/mail/antispam/ for details.

Content preview: [...]

Content analysis details: (5.1 points, 5.0 required)

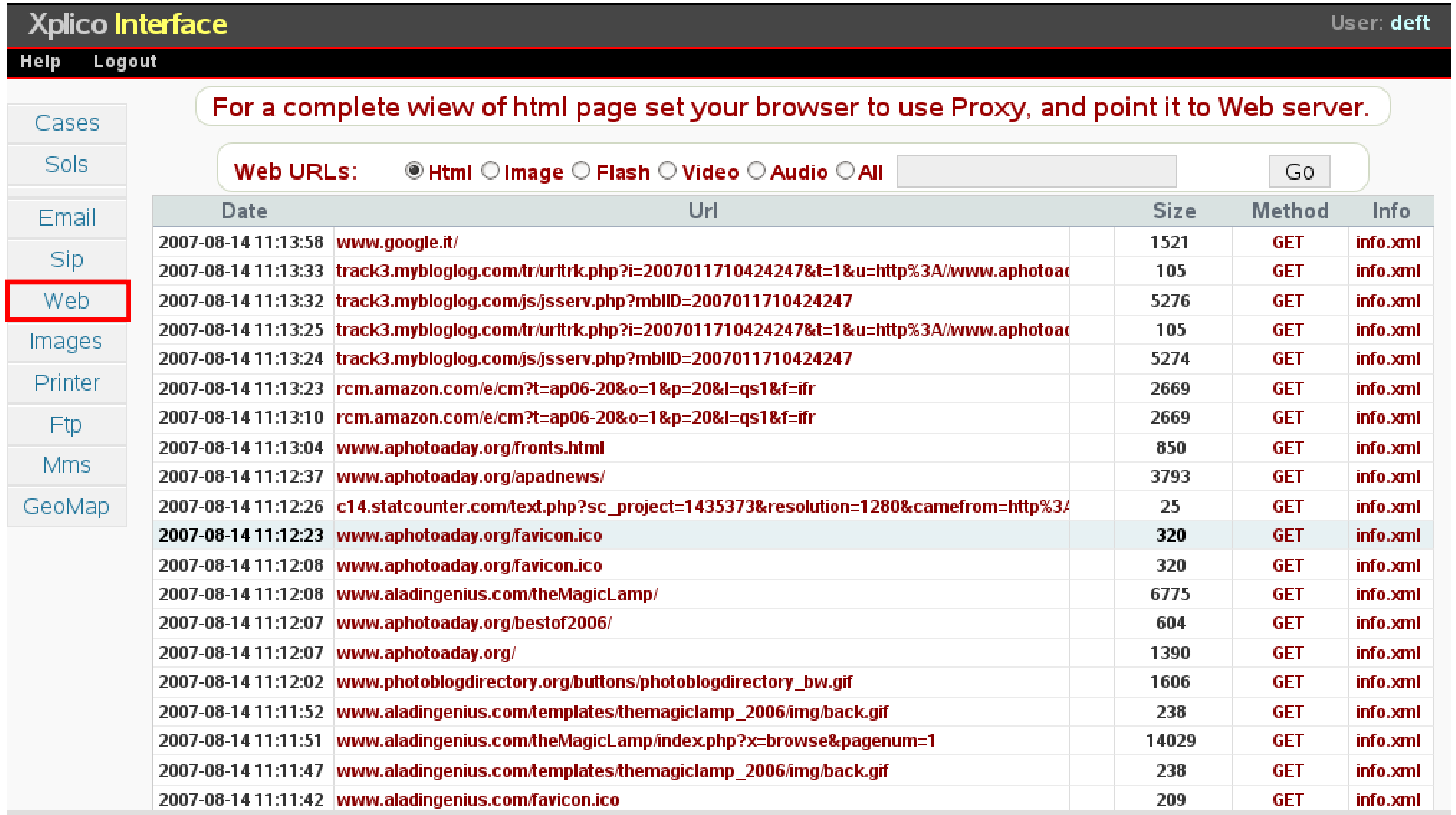
pts rule name description

Attached message E-mail message

© 2007-2009 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

Source: https://www.xplico.org/screenshot

Xplico: Sample HTTP Analysis



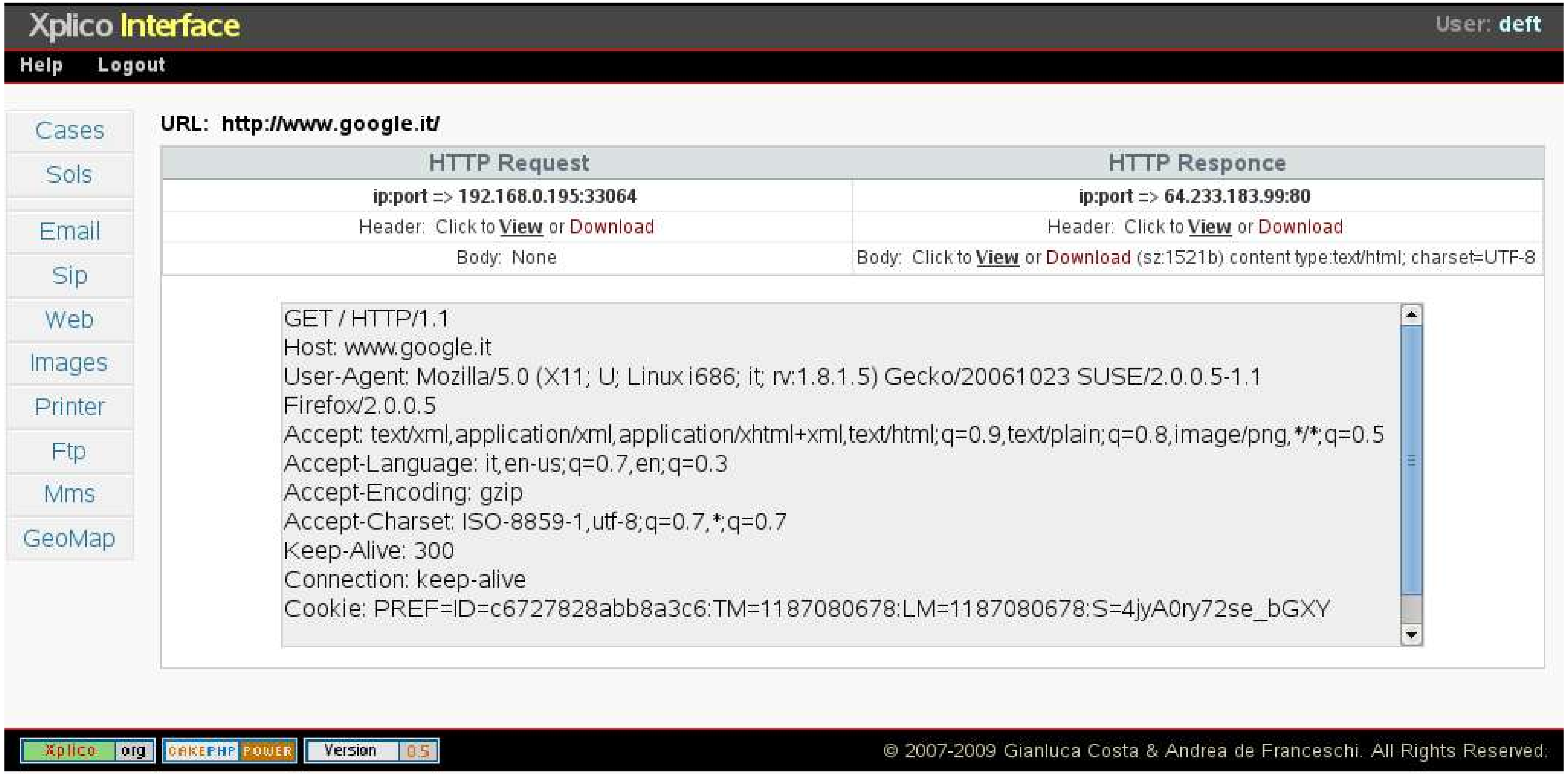
For a complete wiew of html page set your browser to use Proxy, and point it to Web server.

Web URLs: ● Html ○ Image ○ Flash ○ Video ○ Audio ○ All

Date	Url	Size	Method	Info
2007-08-14 11:13:58	www.google.it/	1521	GET	info.xml
2007-08-14 11:13:33	track3.mybloglog.com/tr/urltrk.php?i=2007011710424247&t=1&u=http%3A//www.aphotoac	105	GET	info.xml
2007-08-14 11:13:32	track3.mybloglog.com/js/jsserv.php?mblID=2007011710424247	5276	GET	info.xml
2007-08-14 11:13:25	track3.mybloglog.com/tr/urltrk.php?i=2007011710424247&t=1&u=http%3A//www.aphotoac	105	GET	info.xml
2007-08-14 11:13:24	track3.mybloglog.com/js/jsserv.php?mblID=2007011710424247	5274	GET	info.xml
2007-08-14 11:13:23	rcm.amazon.com/e/cm?t=ap06-20&o=1&p=20&l=qs1&f=ifr	2669	GET	info.xml
2007-08-14 11:13:10	rcm.amazon.com/e/cm?t=ap06-20&o=1&p=20&l=qs1&f=ifr	2669	GET	info.xml
2007-08-14 11:13:04	www.aphotoaday.org/fronts.html	850	GET	info.xml
2007-08-14 11:12:37	www.aphotoaday.org/apadnews/	3793	GET	info.xml
2007-08-14 11:12:26	c14.statcounter.com/text.php?sc_project=1435373&resolution=1280&camefrom=http%3	25	GET	info.xml
2007-08-14 11:12:23	www.aphotoaday.org/favicon.ico	320	GET	info.xml
2007-08-14 11:12:08	www.aphotoaday.org/favicon.ico	320	GET	info.xml
2007-08-14 11:12:08	www.aladingenius.com/theMagicLamp/	6775	GET	info.xml
2007-08-14 11:12:07	www.aphotoaday.org/bestof2006/	604	GET	info.xml
2007-08-14 11:12:07	www.aphotoaday.org/	1390	GET	info.xml
2007-08-14 11:12:02	www.photoblogdirectory.org/buttons/photoblogdirectory_bw.gif	1606	GET	info.xml
2007-08-14 11:11:52	www.aladingenius.com/templates/themagiclamp_2006/img/back.gif	238	GET	info.xml
2007-08-14 11:11:51	www.aladingenius.com/theMagicLamp/index.php?x=browse&pagenum=1	14029	GET	info.xml
2007-08-14 11:11:47	www.aladingenius.com/templates/themagiclamp_2006/img/back.gif	238	GET	info.xml
2007-08-14 11:11:42	www.aladingenius.com/favicon.ico	209	GET	info.xml

Source: https://www.xplico.org/screenshot

Xplico: Sample HTTP Analysis



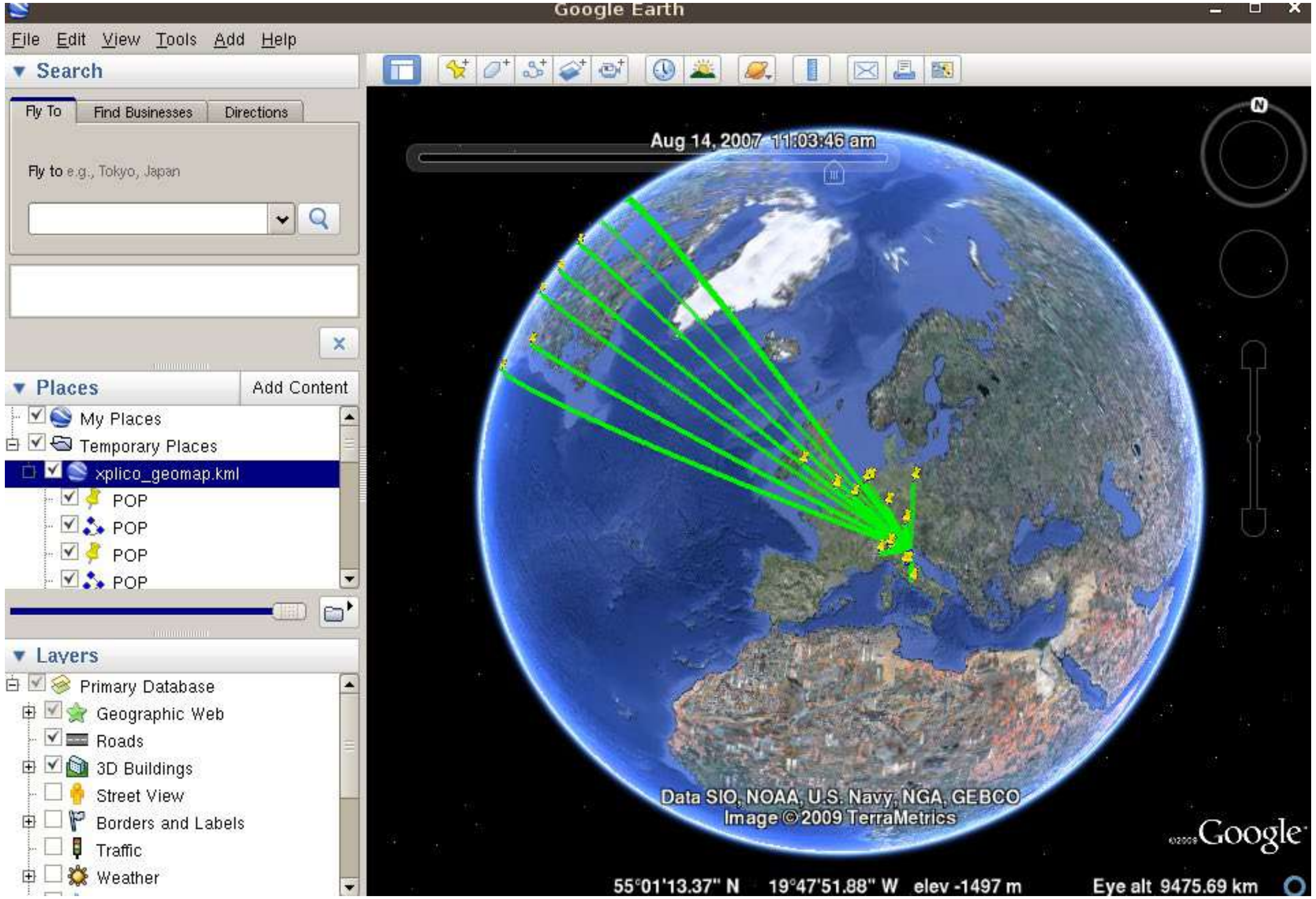
URL: http://www.google.it/

HTTP Request	HTTP Responce
ip:port => 192.168.0.195:33064	ip:port => 64.233.183.99:80
Header: Click to View or Download	Header: Click to View or Download
Body: None	Body: Click to View or Download (sz:1521b) content type:text/html; charset=UTF-8

```
GET / HTTP/1.1
Host: www.google.it
User-Agent: Mozilla/5.0 (X11; U; Linux i686; it; rv:1.8.1.5) Gecko/20061023 SUSE/2.0.0.5-1.1
Firefox/2.0.0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: it,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PREF=ID=c6727828abb8a3c6:TM=1187080678:LM=1187080678:S=4jyA0ry72se_bGXY
```

Source: https://www.xplico.org/screenshot

Xplico: Sample Geomap Analysis



Source: https://www.xplico.org/screenshot

Xplico: References

- **Resources/documentations**:
  - Xplico Wiki: http://wiki.xplico.org/doku.php
  - Russ McRee, "Xplico", ISSA Journal, June 2011: https://holisticinfosec.io/toolsmith/pdf/june2011.pdf

Network Log Analysis

Places Where Network Logs Available

- **Authentication** logs
- **Application** logs
- **OS** logs
- **Networking device** logs:
  - Volatile data
  - Non-volatile data
- **Firewall** logs
- **IDS** logs
- …

Router Log

- ***Volatile*** data:
  - **(Normal) RAM**: holds state tables, e.g. current routing table, listening services, etc.
  - **Non-volatile RAM (NVRAM)**: saves configuration files
- ***Non-volatile*** data:
  - Stored **logs**, **files**, etc.

NetFlow

- ***NetFlow records***: contain a ***summarization*** of network communications seen at a collection point
- But it has ***no traffic content***: just a summary record, including metadata about each network connection
- Less details with **more compact** size:
  - Fewer **privacy concerns** with collecting and storing NetFlow records
  - Longer-term record **retention**
  - **Faster analysis** than full-packet traffic (PCAP) analysis
- Drawback:
  - Detailed low-level analysis and findings may **not** be possible

Review

Firewall: Types of Firewall (Recap)

- **Traditional packet filters**:
  - Applying rules to packets in/out of firewall
  - Based on information in **packet header**
- **Stateful packet filters (SPFs)**:
  - Maintaining a state table of all active connections
  - Filtering packets based on **connection states**
- **Proxy-based firewalls**:
  - Understanding **application logic**
  - Acting as a relay of **application-level traffic**
  - E.g.: **web application firewall (WAF)**:
    an application firewall for HTTP applications

Iptables: Sample Rules of Logging ICMP

```
iptables -t filter -A INPUT -p icmp --icmp-type echo-request -j LOG
--log-prefix="ICMPIN:"

iptables -t filter -A INPUT -p icmp --icmp-type echo-reply -j LOG
--log-prefix="ICMPIN:"

iptables -t filter -A OUTPUT -p icmp --icmp-type echo-request -j LOG
--log-prefix="ICMPOUT:"

iptables -t filter -A OUTPUT -p icmp --icmp-type echo-reply -j LOG
--log-prefix="ICMPOUT:"

iptables -t filter -A FORWARD -p icmp --icmp-type echo-request -j
LOG --log-prefix="ICMPFOR:"

iptables -t filter -A FORWARD -p icmp --icmp-type echo-reply -j LOG
--log-prefix="ICMPFOR:"
```

IDS: Some Definitions

- ***Intrusion Detection*** **(*ID*)**:
  - “The process of **monitoring events** occurring in a computer system or network, and analyzing them for signs of possible ***incidents***”
- ***Incidents***:
  - “**Violations** or imminent **threats of violation** of: computer security policies, acceptable use policies, or standard security practices” [Scarfone & Mell, NIST, 2007]
- ***IDS***:
  - A device or software that automates the **intrusion detection process**

IDS vs IPS, Role

- ***Intrusion Prevention System (IPS)***:
  - Has all the capabilities of an IDS, and can also attempt to ***stop*** possible incidents: **“active” IDS**

- **Role** of an IDS/IPS:
  - As a **second line** of defense
  - Can be thought as a “**burglar alarm**”
  - Complements firewall, anti-virus, etc.

- We will just use the term “IDS” to refer to both IDS & IPS

Snort: Network IDS Mode

- **Snort in NIDS mode**: performs detection & analysis on network traffic

- **Run** using the configuration file **`snort.conf`**:

```
./snort -dev -l ./log -h 192.168.1.0/24
     -c snort.conf
```

- Default **output** directory: **`/var/log/snort`**

- Sample Snort **alert message**:

```
[**] [116:56:1] (snort_decoder): T/TCP Detected [**]
```

- **Three shown numbers**: *Generator ID* (e.g. decode/116 component), *Snort/Signature ID* (e.g. 56 as a T/TCP event), *Revision ID* (e.g. 1)

Snort Rules & Rule Components

- Sample **Snort rules**:

```
alert tcp any any -> any any (flags:0; msg:"Null Scan";)

alert tcp any any -> 192.169.1.0/24 111 (content:"|00 01 86
a5|"; msg:"mountd access";)
```

- **Rule action**:
  - **Options**: **`alert`**, **`log`**, `pass`, `activate`, `dynamic`
  - Additional options when running as **NIPS**: `drop`, `reject`, `sdrop`
- Protocol: `tcp`, `udp`, `icmp`, `ip`
- Source IP address
- Source port no

Snort Rules & Rule Components

- Sample **Snort rules**:

```
alert tcp any any -> any any (flags:0; msg:"Null Scan";)

alert tcp any any -> 192.169.1.0/24 111 (content:"|00 01
86 a5|"; msg:"mountd access";)
```

- Direction operator: **->, <>** (there is no <-)
- Destination IP address
- Destination port no
- Rule option classes: non-payload (e.g. `flags`), payload (e.g. `content`), general (e.g. **`msg`**), and post-detection (e.g. `replace`) classes

Network Forensics: Resources

Books (both ebooks are available from NUS Libraries) & **article**:

- Ric Messier, “*Network Forensics*”, Wiley, 2017
- Jessey Bullock and Jeff Parker, “*Wireshark for Security Professionals : Using Wireshark and the Metasploit Framework*”, Wiley, 2017
- Russ McRee, "*Security Analysis with Wireshark*", https://holisticinfosec.io/toolsmith/pdf/november2006.pdf

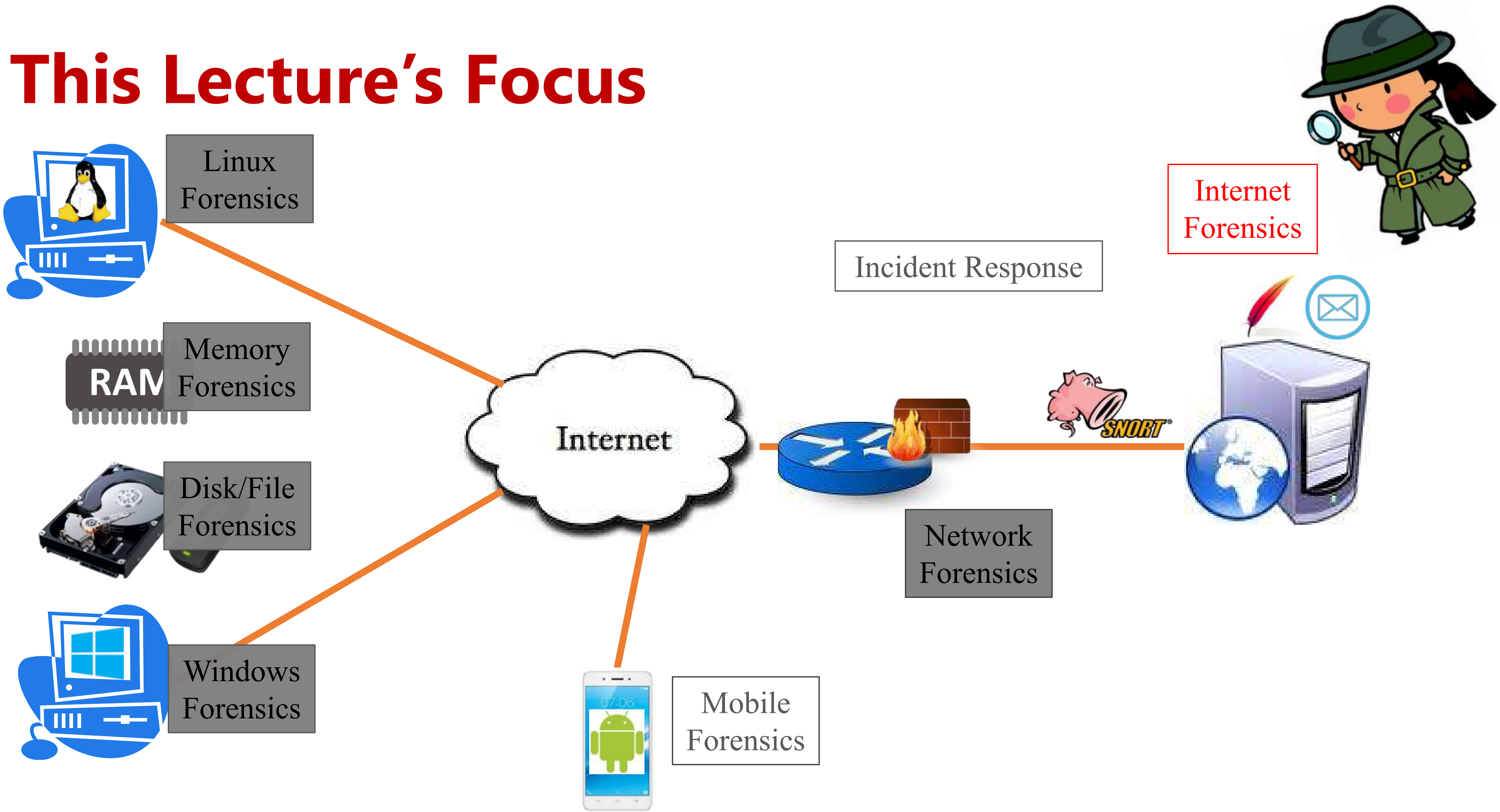
Video:

- Wireshark filtering: https://www.youtube.com/watch?v=rlDIIgzyo1Y

Break!

Internet Forensics

This Lecture's Focus



Internet Forensics

- Below are some ***Internet artefacts***: generated by **Internet applications**
- ***Browser artefacts***:
  - Browser **cache**
  - Browser **history**: history file(s)/database, registry entries (Windows)
  - **Cookies**
  - **Stored passwords**
  - **Downloads**
  - **Bookmarks**
  - Installed browser **extensions**
- ***Email artefacts***:
  - Sent email **headers** and **message bodies**
  - Stored **mailbox files**: MS Outlook PST/OST files, OLK folder
  - Logs on **email servers**
- *Others: from other Internet applications*

Web Artefacts

Browser Artefacts

- Browser artefacts:
  - *A **very good*** **source** of computer forensic evidence
  - Record **Internet activities** of web users, including:
    - **Typed & visited URLs**
    - **Search activity**
    - **Web sessions (cookies)**
    - **Stored passwords**
    - **Download activity**
    - …
  - Can be recovered from the **deleted space**!
- Video on browser forensics: https://www.youtube.com/watch?v=WVb-vkaw6DI

Web *History*

- Records ***websites visited*** by date and time
- Stored for each **local user account**
- Web history **file locations**:
  - **Chrome (XP)**: %USERPROFILE%`\Local Settings\Application Data\Google\Chrome\User Data\Default\History`
  - **Chrome (Win 7/8/10)**: %USERPROFILE%`\`**`AppData`**`\Local\Google\Chrome\User Data\Default\History`
  - **Firefox (XP)**: %USERPROFILE%`\Application Data\Mozilla\Firefox\Profiles\`<random text>`.default\places.sqlite`
  - **Firefox (Win 7/8/10)**: %USERPROFILE%`\`**`AppData`**`\Roaming\Mozilla\Firefox\Profiles\`<random text>`.default\places.sqlite`

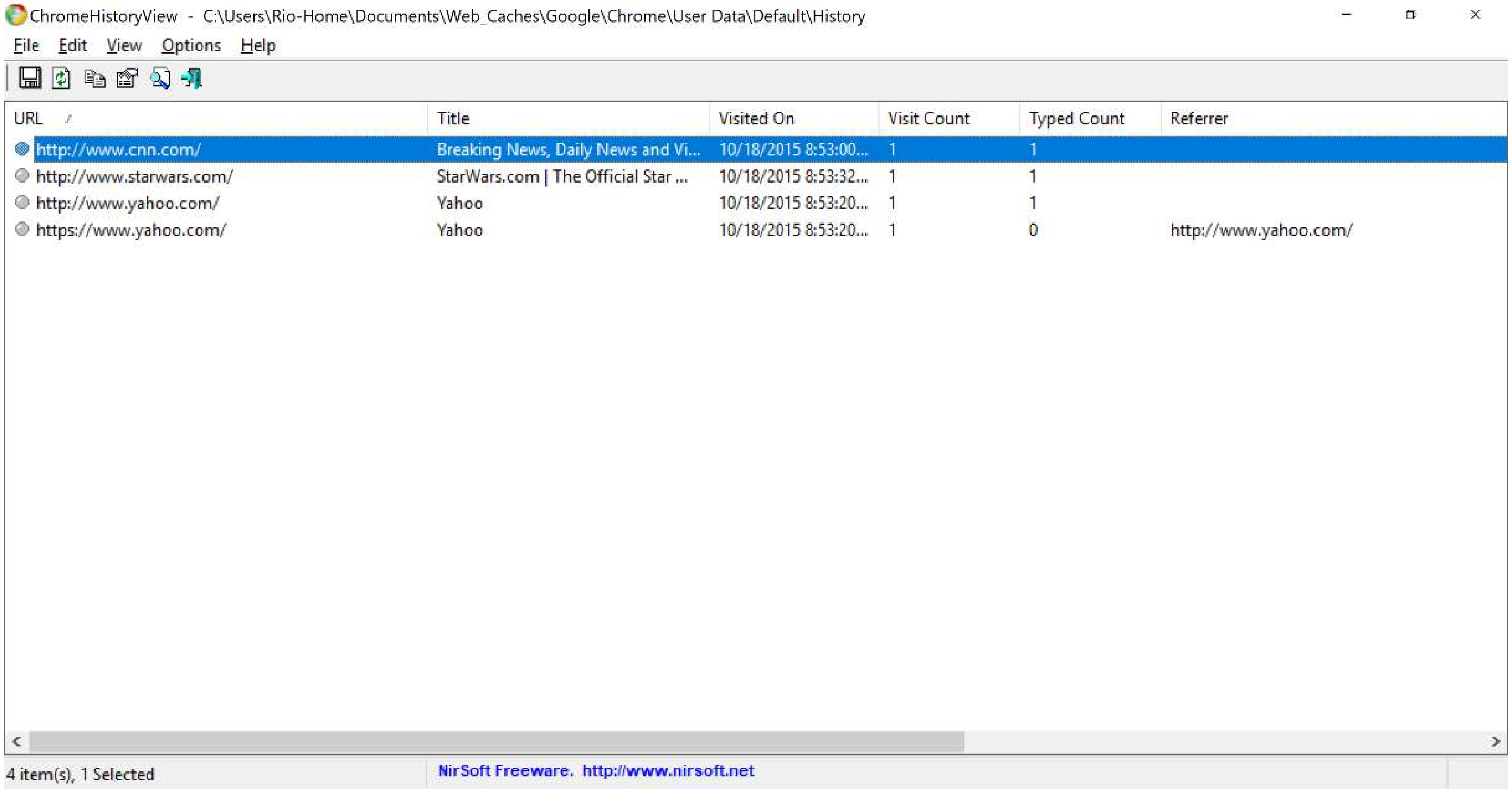
Web *Cache*

- Stores ***webpage components*** to speed up subsequent visits
- Folder **locations**:
  - **Chrome (XP)**: %USERPROFILE%`\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache`
  - **Chrome (Win 7/8/10)**: %USERPROFILE%`\`**`AppData`**`\Local\Google\Chrome\User Data\Default\Cache`
  - **Firefox (XP)**: %USERPROFILE%`\Local Settings\ApplicationData\Mozilla\Firefox\Profiles\`<*random-text*>`.default\Cache`
  - **Firefox (Win 7/8/10)**: %USERPROFILE%`\`**`AppData`**`\Local\Mozilla\Firefox\Profiles\`<*random-text*>`.default\Cache`

Some Useful Tools for Browser Artefacts

- Tools (from **NirSoft**): see **Lab 7**
    - ChromeHistoryView (CHV)
    - ChromeCacheView (CCV)
    - MozillaHistoryView (MHV)
    - MozillaCacheView (MCV)
    - …

NirSoft’s ChromeHistoryView



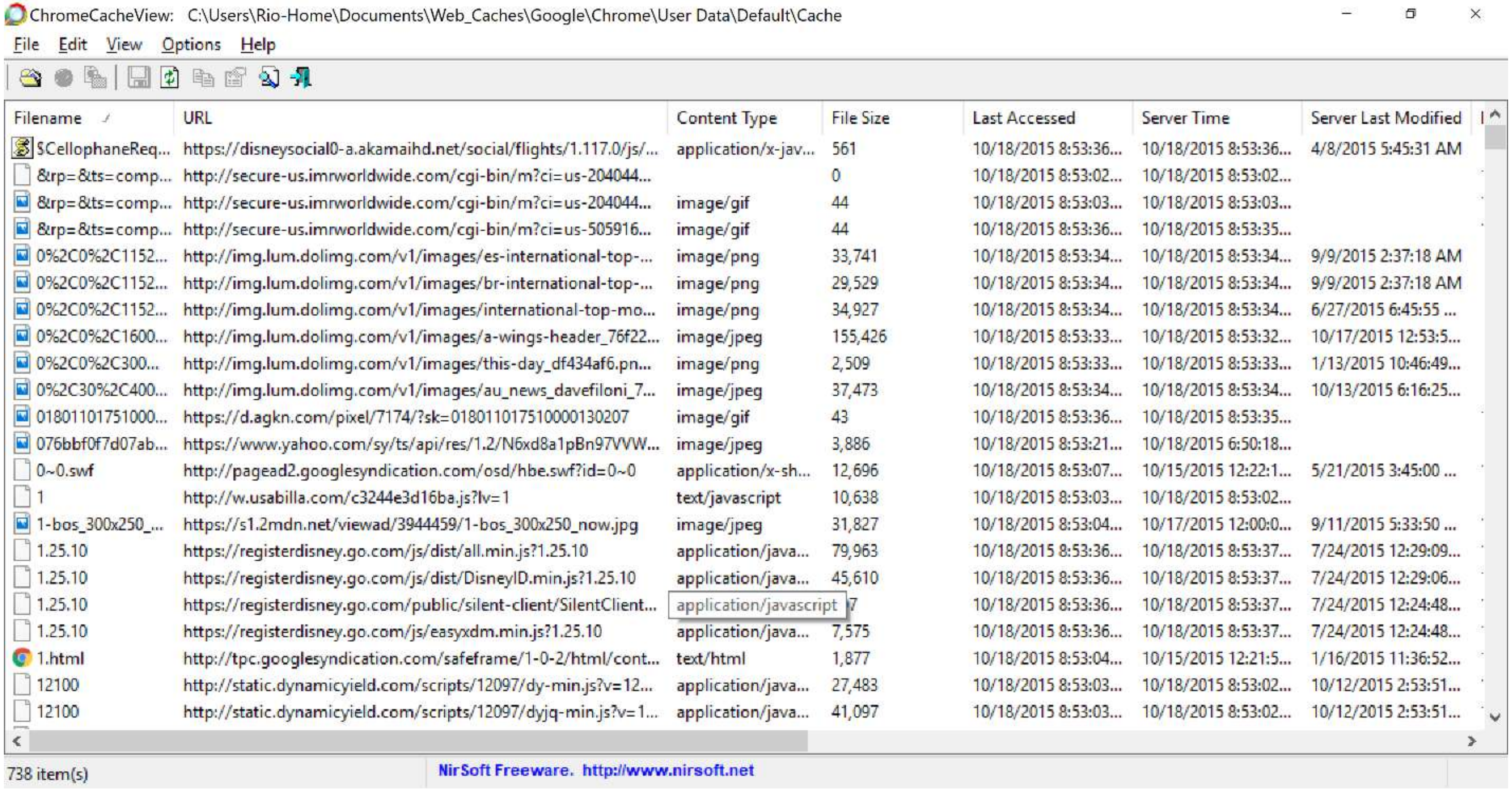
ChromeHistoryView - C:\Users\Rio-Home\Documents\Web_Caches\Google\Chrome\User Data\Default\History
File Edit View Options Help

URL	Title	Visited On	Visit Count	Typed Count	Referrer
http://www.cnn.com/	Breaking News, Daily News and Vi...	10/18/2015 8:53:00...	1	1	
http://www.starwars.com/	StarWars.com | The Official Star ...	10/18/2015 8:53:32...	1	1	
http://www.yahoo.com/	Yahoo	10/18/2015 8:53:20...	1	1	
https://www.yahoo.com/	Yahoo	10/18/2015 8:53:20...	1	0	http://www.yahoo.com/

4 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

NirSoft’s ChromeCacheView



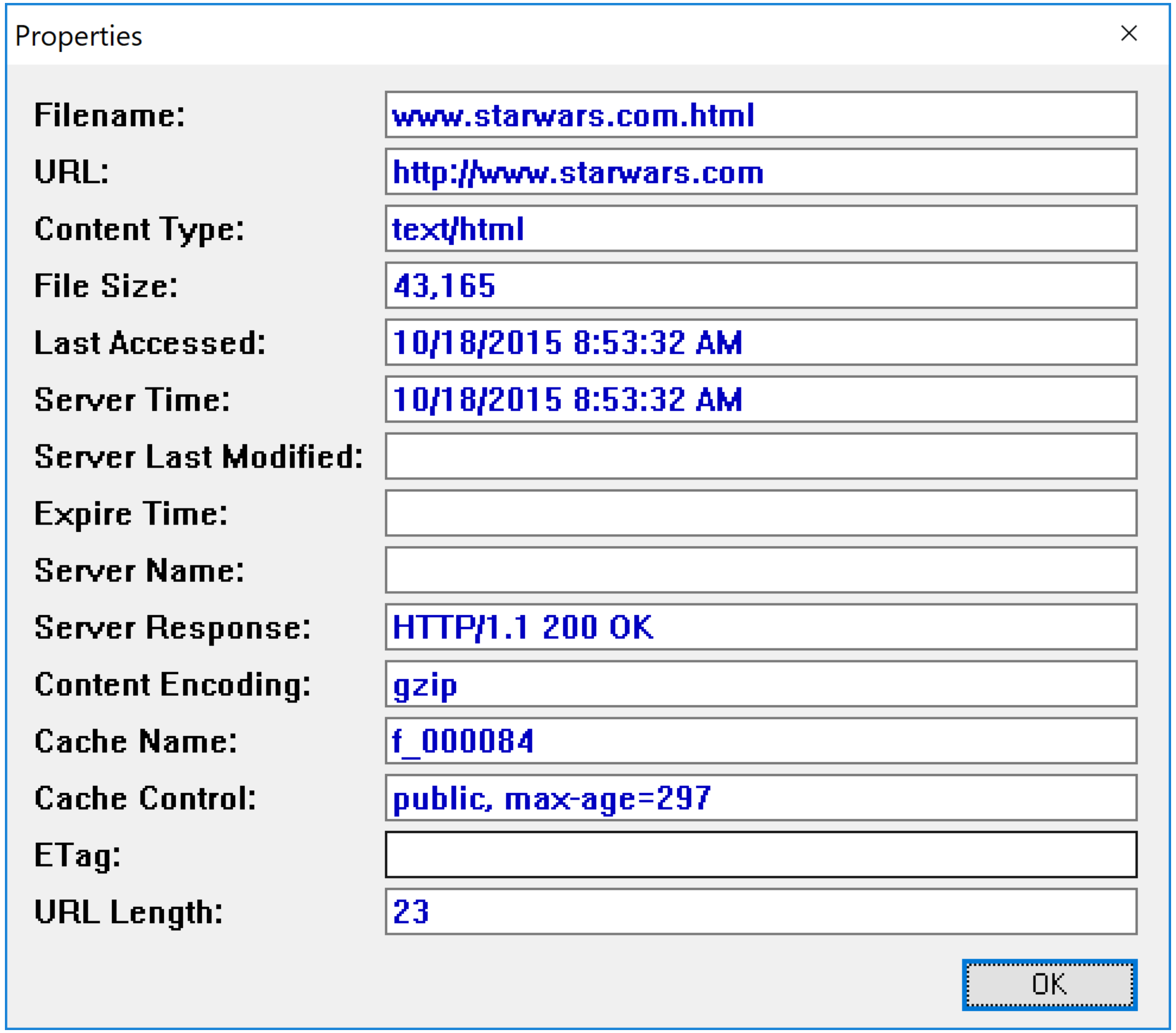
ChromeCacheView: C:\Users\Rio-Home\Documents\Web_Caches\Google\Chrome\User Data\Default\Cache
File Edit View Options Help

Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified
$CellophaneReq...	https://disneysocial0-a.akamaihd.net/social/flights/1.117.0/js/...	application/x-jav...	561	10/18/2015 8:53:36...	10/18/2015 8:53:36...	4/8/2015 5:45:31 AM
&rp=&ts=comp...	http://secure-us.imrworldwide.com/cgi-bin/m?ci=us-204044...		0	10/18/2015 8:53:02...	10/18/2015 8:53:02...	
&rp=&ts=comp...	http://secure-us.imrworldwide.com/cgi-bin/m?ci=us-204044...	image/gif	44	10/18/2015 8:53:03...	10/18/2015 8:53:03...	
&rp=&ts=comp...	http://secure-us.imrworldwide.com/cgi-bin/m?ci=us-505916...	image/gif	44	10/18/2015 8:53:36...	10/18/2015 8:53:35...	
0%2C0%2C1152...	http://img.lum.dolimg.com/v1/images/es-international-top-...	image/png	33,741	10/18/2015 8:53:34...	10/18/2015 8:53:34...	9/9/2015 2:37:18 AM
0%2C0%2C1152...	http://img.lum.dolimg.com/v1/images/br-international-top-...	image/png	29,529	10/18/2015 8:53:34...	10/18/2015 8:53:34...	9/9/2015 2:37:18 AM
0%2C0%2C1152...	http://img.lum.dolimg.com/v1/images/international-top-mo...	image/png	34,927	10/18/2015 8:53:34...	10/18/2015 8:53:34...	6/27/2015 6:45:55 ...
0%2C0%2C1600...	http://img.lum.dolimg.com/v1/images/a-wings-header_76f22...	image/jpeg	155,426	10/18/2015 8:53:33...	10/18/2015 8:53:32...	10/17/2015 12:53:5...
0%2C0%2C300...	http://img.lum.dolimg.com/v1/images/this-day_df434af6.pn...	image/png	2,509	10/18/2015 8:53:33...	10/18/2015 8:53:33...	1/13/2015 10:46:49...
0%2C30%2C400...	http://img.lum.dolimg.com/v1/images/au_news_davefiloni_7...	image/jpeg	37,473	10/18/2015 8:53:34...	10/18/2015 8:53:34...	10/13/2015 6:16:25...
01801101751000...	https://d.agkn.com/pixel/7174/?sk=01801101751000130207	image/gif	43	10/18/2015 8:53:36...	10/18/2015 8:53:35...	
076bbf0f7d07ab...	https://www.yahoo.com/sy/ts/api/res/1.2/N6xd8a1pBn97VVW...	image/jpeg	3,886	10/18/2015 8:53:21...	10/18/2015 6:50:18...	
0~0.swf	http://pagead2.googlesyndication.com/osd/hbe.swf?id=0~0	application/x-sh...	12,696	10/18/2015 8:53:07...	10/15/2015 12:22:1...	5/21/2015 3:45:00 ...
1	http://w.usabilla.com/c3244e3d16ba.js?lv=1	text/javascript	10,638	10/18/2015 8:53:03...	10/18/2015 8:53:02...	
1-bos_300x250_...	https://s1.2mdn.net/viewad/3944459/1-bos_300x250_now.jpg	image/jpeg	31,827	10/18/2015 8:53:04...	10/17/2015 12:00:0...	9/11/2015 5:33:50 ...
1.25.10	https://registerdisney.go.com/js/dist/all.min.js?1.25.10	application/java...	79,963	10/18/2015 8:53:36...	10/18/2015 8:53:37...	7/24/2015 12:29:09...
1.25.10	https://registerdisney.go.com/js/dist/DisneyID.min.js?1.25.10	application/java...	45,610	10/18/2015 8:53:36...	10/18/2015 8:53:37...	7/24/2015 12:29:06...
1.25.10	https://registerdisney.go.com/public/silent-client/SilentClient...	application/javascript	7	10/18/2015 8:53:36...	10/18/2015 8:53:37...	7/24/2015 12:24:48...
1.25.10	https://registerdisney.go.com/js/easyxdm.min.js?1.25.10	application/java...	7,575	10/18/2015 8:53:36...	10/18/2015 8:53:37...	7/24/2015 12:24:48...
1.html	http://tpc.googlesyndication.com/safeframe/1-0-2/html/cont...	text/html	1,877	10/18/2015 8:53:04...	10/15/2015 12:21:5...	1/16/2015 11:36:52...
12100	http://static.dynamicyield.com/scripts/12097/dy-min.js?v=12...	application/java...	27,483	10/18/2015 8:53:03...	10/18/2015 8:53:02...	10/12/2015 2:53:51...
12100	http://static.dynamicyield.com/scripts/12097/dyjq-min.js?v=1...	application/java...	41,097	10/18/2015 8:53:03...	10/18/2015 8:53:02...	10/12/2015 2:53:51...

738 item(s)

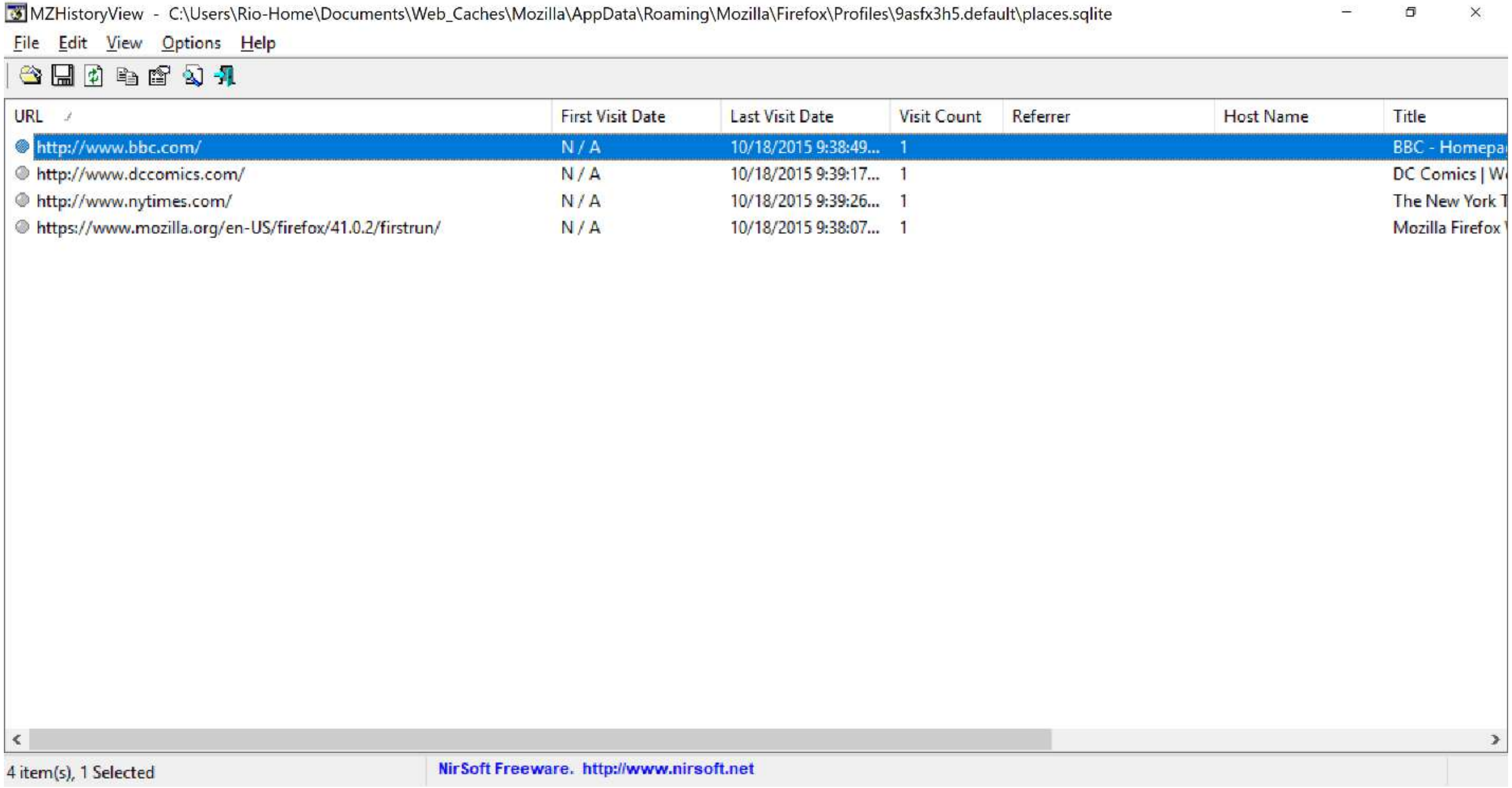
NirSoft Freeware. http://www.nirsoft.net

NirSoft’s ChromeCacheView



Filename:	www.starwars.com.html
URL:	http://www.starwars.com
Content Type:	text/html
File Size:	43,165
Last Accessed:	10/18/2015 8:53:32 AM
Server Time:	10/18/2015 8:53:32 AM
Server Last Modified:	
Expire Time:	
Server Name:	
Server Response:	HTTP/1.1 200 OK
Content Encoding:	gzip
Cache Name:	f_000084
Cache Control:	public, max-age=297
ETag:	
URL Length:	23

NirSoft's MozillaHistoryView



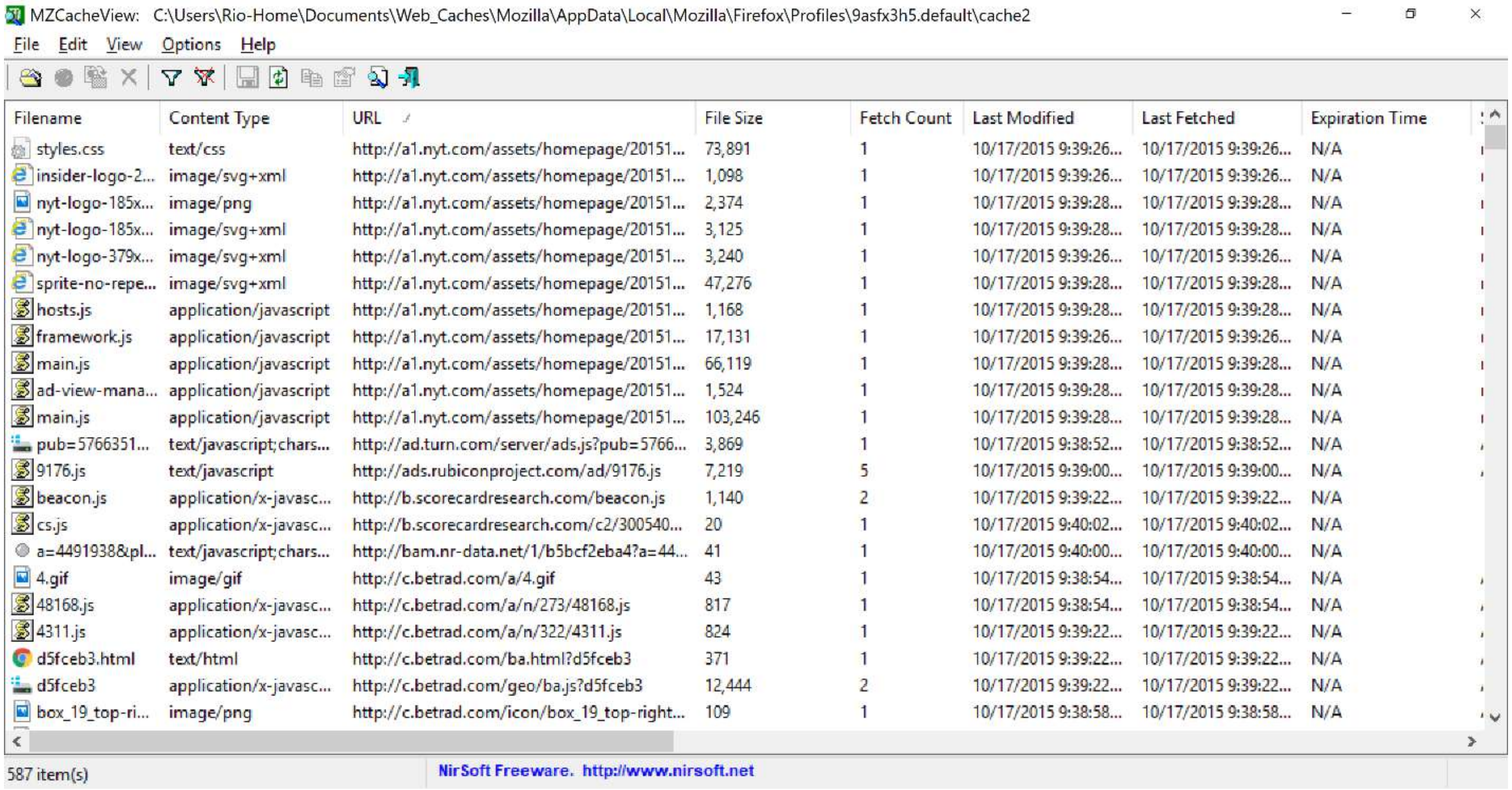
MZHistoryView - C:\Users\Rio-Home\Documents\Web_Caches\Mozilla\AppData\Roaming\Mozilla\Firefox\Profiles\9asfx3h5.default\places.sqlite
File
Edit
View
Options
Help

URL	First Visit Date	Last Visit Date	Visit Count	Referrer	Host Name	Title
http://www.bbc.com/	N / A	10/18/2015 9:38:49...	1			BBC - Homepa
http://www.dccomics.com/	N / A	10/18/2015 9:39:17...	1			DC Comics | W
http://www.nytimes.com/	N / A	10/18/2015 9:39:26...	1			The New York T
https://www.mozilla.org/en-US/firefox/41.0.2/firstrun/	N / A	10/18/2015 9:38:07...	1			Mozilla Firefox

4 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

NirSoft's MozillaCacheView



MZCacheView: C:\Users\Rio-Home\Documents\Web_Caches\Mozilla\AppData\Local\Mozilla\Firefox\Profiles\9asfx3h5.default\cache2
File
Edit
View
Options
Help

Filename	Content Type	URL	File Size	Fetch Count	Last Modified	Last Fetched	Expiration Time
styles.css	text/css	http://a1.nyt.com/assets/homepage/20151...	73,891	1	10/17/2015 9:39:26...	10/17/2015 9:39:26...	N/A
insider-logo-2...	image/svg+xml	http://a1.nyt.com/assets/homepage/20151...	1,098	1	10/17/2015 9:39:26...	10/17/2015 9:39:26...	N/A
nyt-logo-185x...	image/png	http://a1.nyt.com/assets/homepage/20151...	2,374	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
nyt-logo-185x...	image/svg+xml	http://a1.nyt.com/assets/homepage/20151...	3,125	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
nyt-logo-379x...	image/svg+xml	http://a1.nyt.com/assets/homepage/20151...	3,240	1	10/17/2015 9:39:26...	10/17/2015 9:39:26...	N/A
sprite-no-repe...	image/svg+xml	http://a1.nyt.com/assets/homepage/20151...	47,276	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
hosts.js	application/javascript	http://a1.nyt.com/assets/homepage/20151...	1,168	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
framework.js	application/javascript	http://a1.nyt.com/assets/homepage/20151...	17,131	1	10/17/2015 9:39:26...	10/17/2015 9:39:26...	N/A
main.js	application/javascript	http://a1.nyt.com/assets/homepage/20151...	66,119	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
ad-view-mana...	application/javascript	http://a1.nyt.com/assets/homepage/20151...	1,524	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
main.js	application/javascript	http://a1.nyt.com/assets/homepage/20151...	103,246	1	10/17/2015 9:39:28...	10/17/2015 9:39:28...	N/A
pub=5766351...	text/javascript;chars...	http://ad.turn.com/server/ads.js?pub=5766...	3,869	1	10/17/2015 9:38:52...	10/17/2015 9:38:52...	N/A
9176.js	text/javascript	http://ads.rubiconproject.com/ad/9176.js	7,219	5	10/17/2015 9:39:00...	10/17/2015 9:39:00...	N/A
beacon.js	application/x-javasc...	http://b.scorecardresearch.com/beacon.js	1,140	2	10/17/2015 9:39:22...	10/17/2015 9:39:22...	N/A
cs.js	application/x-javasc...	http://b.scorecardresearch.com/c2/300540...	20	1	10/17/2015 9:40:02...	10/17/2015 9:40:02...	N/A
a=4491938&pl...	text/javascript;chars...	http://bam.nr-data.net/1/b5bcf2eba4?a=44...	41	1	10/17/2015 9:40:00...	10/17/2015 9:40:00...	N/A
4.gif	image/gif	http://c.betrad.com/a/4.gif	43	1	10/17/2015 9:38:54...	10/17/2015 9:38:54...	N/A
48168.js	application/x-javasc...	http://c.betrad.com/a/n/273/48168.js	817	1	10/17/2015 9:38:54...	10/17/2015 9:38:54...	N/A
4311.js	application/x-javasc...	http://c.betrad.com/a/n/322/4311.js	824	1	10/17/2015 9:39:22...	10/17/2015 9:39:22...	N/A
d5fceb3.html	text/html	http://c.betrad.com/ba.html?d5fceb3	371	1	10/17/2015 9:39:22...	10/17/2015 9:39:22...	N/A
d5fceb3	application/x-javasc...	http://c.betrad.com/geo/ba.js?d5fceb3	12,444	2	10/17/2015 9:39:22...	10/17/2015 9:39:22...	N/A
box_19_top-ri...	image/png	http://c.betrad.com/icon/box_19_top-right...	109	1	10/17/2015 9:38:58...	10/17/2015 9:38:58...	N/A

587 item(s)

NirSoft Freeware. http://www.nirsoft.net

Cookies

- Tells ***visited websites*** and ***session*** details
- **Folder/file Location**:
  - **Chrome (XP)**: %USERPROFILE%`\Local Settings\ApplicationData\Google\Chrome\User Data\Default\Local Storage`
  - **Chrome (Win7/8/10)**: %USERPROFILE%`\AppData\Local\Google\Chrome\User Data\Default\Local Storage`
  - **Firefox (XP)**: %USERPROFILE%`\Application Data\Mozilla\Firefox\Profiles\`<random text>`.default\cookies.sqlite`
  - **Firefox (Win7/8/10)**: %USERPROFILE%`\AppData\Roaming\Mozilla\Firefox\Profiles\`<random text>`.default\cookies.sqlite`

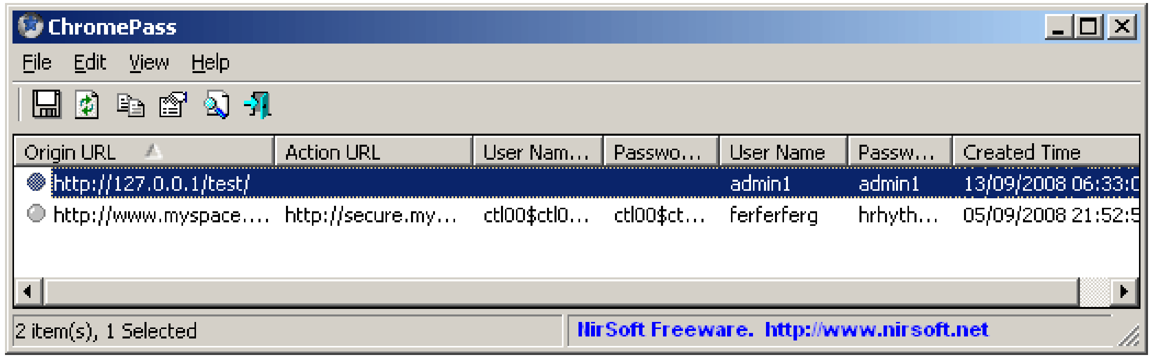
Some Useful Tools

- **Cookie** extraction/view tools (from NirSoft):
  - **ChromeCookiesView:** https://www.nirsoft.net/utils/chrome_cookies_view.html
  - **MZCookiesView:** https://www.nirsoft.net/utils/mzcv.html
  - **IECookiesView:** https://www.nirsoft.net/utils/iecookies.html

Browser's *Stored Passwords*

- Website login ***passwords/credentials*** stored by browsers
- Stored for each **user profile** based on the user's consent
- Usually stored **encrypted**
- Yet, tools are available to **extract/recover** the stored credentials:
    - **ChromePass**: https://www.nirsoft.net/utils/chromepass.html
    - **PasswordFox**: https://www.nirsoft.net/utils/passwordfox.html
    - **IE PassView**: https://www.nirsoft.net/utils/internet_explorer_password.html

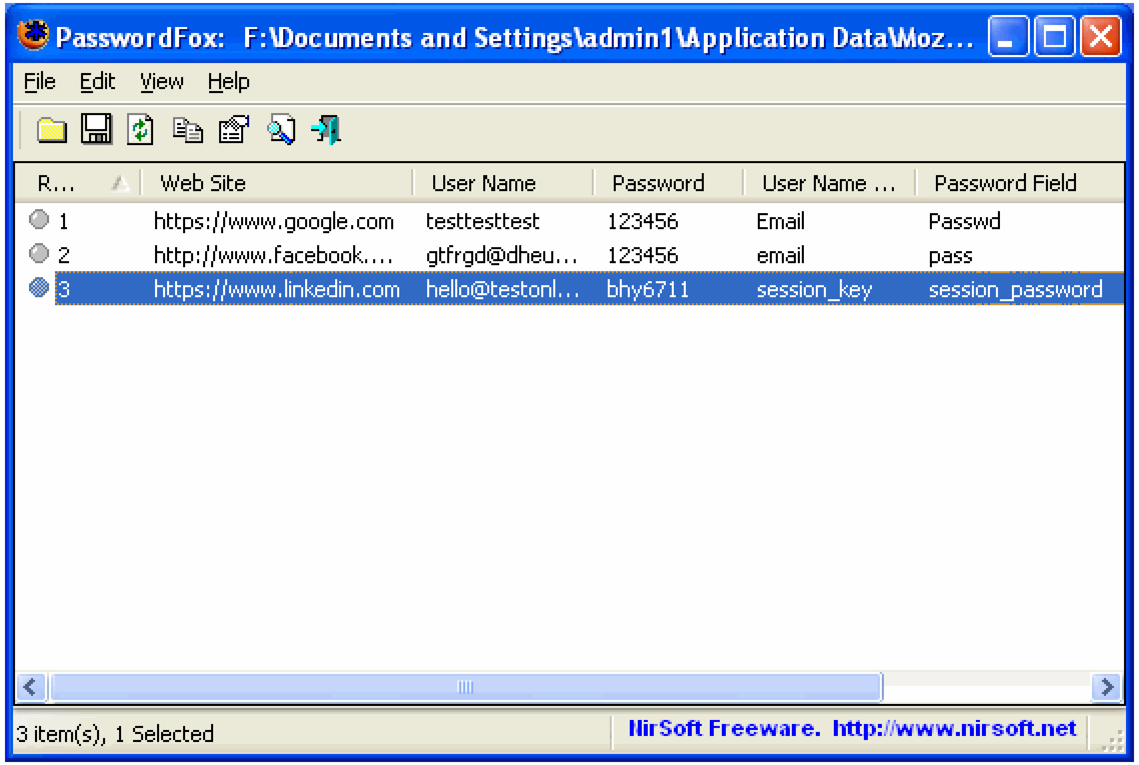
ChromePass & PasswordFox



Origin URL	Action URL	User Nam...	Passwo...	User Name	Passw...	Created Time
http://127.0.0.1/test/				admin1	admin1	13/09/2008 06:33:0
http://www.myspace....	http://secure.my...	ctl00$ctl0...	ctl00$ct...	ferferferg	hrhyth...	05/09/2008 21:52:5

2 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net


PasswordFox: F:\Documents and Settings\admin1\Application Data\Moz...
File Edit View Help

R...	Web Site	User Name	Password	User Name ...	Password Field
1	https://www.google.com	testtesttest	123456	Email	Passwd
2	http://www.facebook....	gtfrgd@dheu...	123456	email	pass
3	https://www.linkedin.com	hello@testonl...	bhy6711	session_key	session_password

3 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

Source:
https://www.nirsoft.net

Web *Downloads*

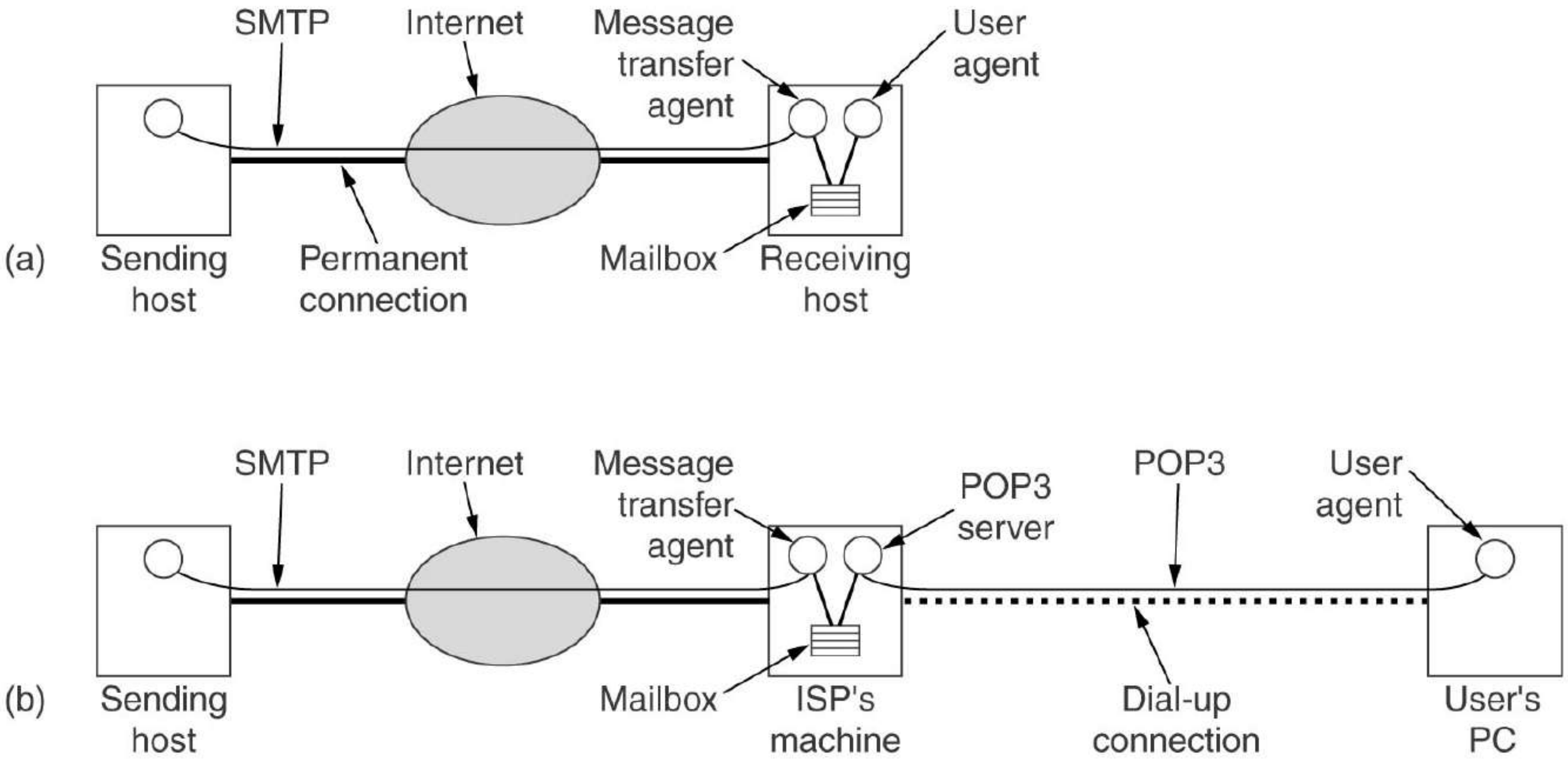
- Some browsers, e.g. Firefox, have a built-in ***download manager*** application
- It keeps a history of **every file downloaded** by web user
- An excellent **source of information** on sites a user has been visiting, what kinds of files they have been downloading from them
- **File locations** (Firefox):
  - **XP**: %userprofile%`\AppData\Local\Mozilla\Firefox\Profiles\`<random text>`.default\downloads.sqlite`
  - **Win7/8/10**: %userprofile%`\AppData\Roaming\Mozilla\ Firefox\Profiles\`<random text>`.default\downloads.sqlite`

Email Artefacts

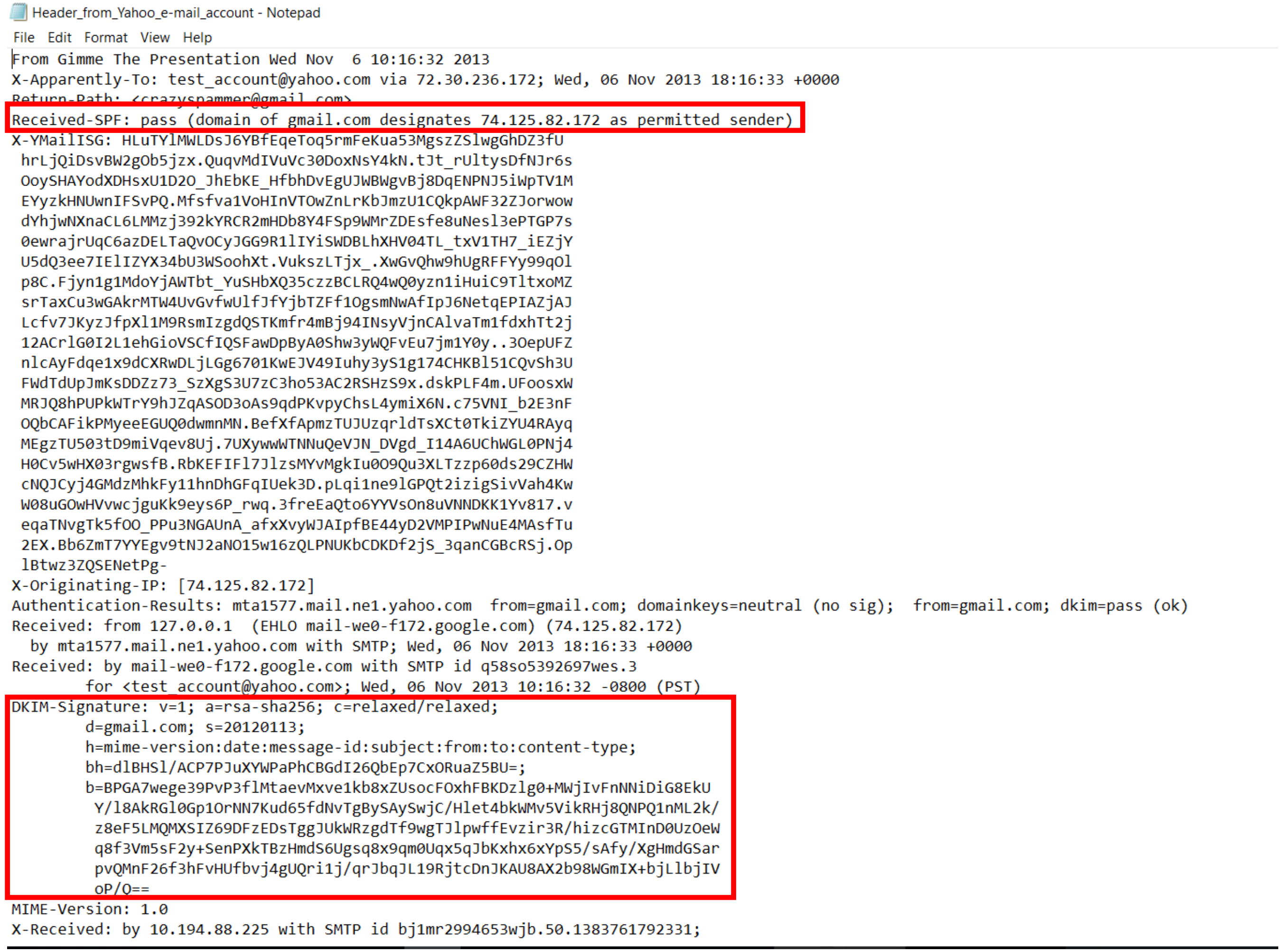
Email Forensics: Some Protocols

- Simple Message Transfer Protocol (**SMTP**): for email transmission
  - Uses IP
  - Contains sender **IP address** & other valuable data in the **header**
- Multipurpose Internet Mail Extensions (**MIME**):
  - Allows other non-text data to be included in the email as **attachements**
- **POP** & **IMAP** email access protocols:
  messages can be kept in user **mailbox file(s)**
- **Webmail**: relevant browser artefacts

SMTP & POP3 Email



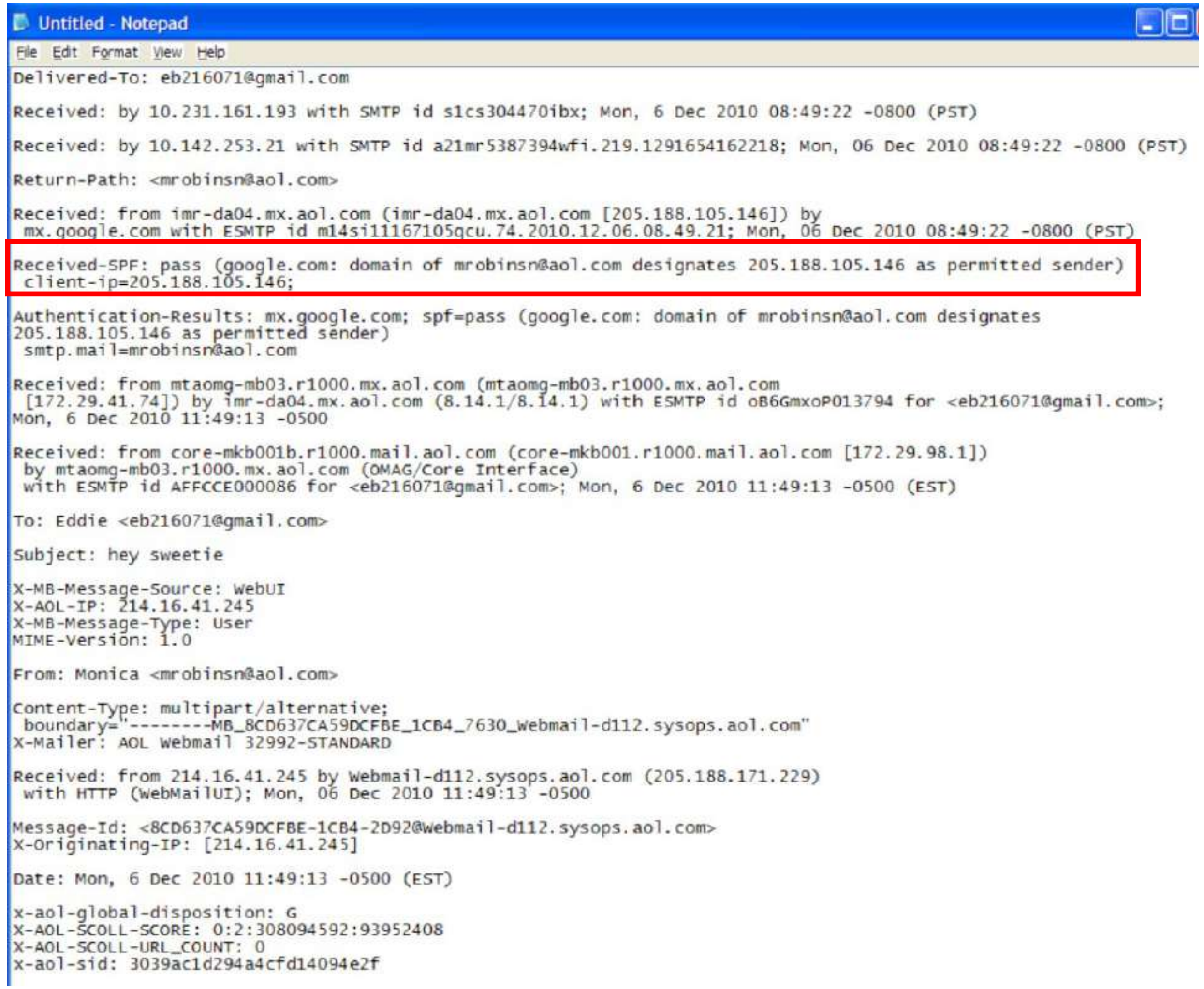
Email Header Analysis: Yahoo Email



Header_from_Yahoo_e-mail_account - Notepad
File Edit Format View Help

```
From Gimme The Presentation Wed Nov  6 10:16:32 2013
X-Apparently-To: test_account@yahoo.com via 72.30.236.172; Wed, 06 Nov 2013 18:16:33 +0000
Return-Path: <crazyspammer@gmail.com>
Received-SPF: pass (domain of gmail.com designates 74.125.82.172 as permitted sender)
X-YMailISG: HLuTYlMWLDsJ6YBfEqeToq5rmFeKua53MgszZSlwgGhDZ3fU
 hrLjQiDsvBW2gOb5jzx.QuqvMdIVuVc30DoxNsY4kN.tJt_rUltysDfNJr6s
 OoySHAYodXDHsxU1D2O_JhEbKE_HfbhDvEgUJWBWgvBj8DqENPNJ5iWpTV1M
 EYyzkHNUwnIFSvPQ.Mfsfva1VoHInVTOwZnLrKbJmzU1CQkpAWF32ZJorwow
 dYhjwNXnaCL6LMMzj392kYRCR2mHDb8Y4FSp9WMrZDEsfe8uNesl3ePTGP7s
 0ewrajrUqC6azDELTaQvOCyJGG9R1lIYiSWDBLhXHV04TL_txV1TH7_iEZjY
 U5dQ3ee7IElIZYX34bU3WSoohXt.VukszLTjx_.XwGvQhw9hUgRFFYy99qOl
 p8C.Fjyn1g1MdoYjAWTbt_YuSHbXQ35czzBCLRQ4wQ0yzn1iHuiC9TltxoMZ
 srTaxCu3wGAkrMTW4UvGvfwUlfJfYjbTZFf1OgsmNwAfIpJ6NetqEPIAZjAJ
 Lcfv7JKyzJfpXl1M9RsmIzgdQSTKmfr4mBj94INsyVjnCAlvaTm1fdxhTt2j
 12ACrlG0I2L1ehGioVSCfIQSFawDpByA0Shw3yWQFvEu7jm1Y0y..3OepUFZ
 nlcAyFdqe1x9dCXRwDLjLGg6701KwEJV49Iuhy3yS1g174CHKBl51CQvSh3U
 FWdTdUpJmKsDDZz73_SzXgS3U7zC3ho53AC2RSHzS9x.dskPLF4m.UFoosxW
 MRJQ8hPUPkWTrY9hJZqASOD3oAs9qdPKvpyChsL4ymiX6N.c75VNI_b2E3nF
 OQbCAFikPMyeeEGUQ0dwmnMN.BefXfApmzTUJUzqrldTsXCt0TkiZYU4RAyq
 MEgzTU5O3tD9miVqev8Uj.7UXywwWTNNuQeVJN_DVgd_I14A6UChWGL0PNj4
 H0Cv5wHX03rgwsfB.RbKEFIFl7JlzsMYvMgkIu0O9Qu3XLTzzp60ds29CZHW
 cNQJCyj4GMdzMhkFy11hnDhGFqIUek3D.pLqi1ne9lGPQt2izigSivVah4Kw
 W08uGOwHVvwcjguKk9eys6P_rwq.3freEaQto6YYVsOn8uVNNDKK1Yv817.v
 eqaTNvgTk5fOO_PPu3NGAUnA_afxXvyWJAIpfBE44yD2VMPIPwNuE4MAsfTu
 2EX.Bb6ZmT7YYEgv9tNJ2aNO15w16zQLPNUKbCDKDf2jS_3qanCGBcRSj.Op
 lBtwz3ZQSENetPg-
X-Originating-IP: [74.125.82.172]
Authentication-Results: mta1577.mail.ne1.yahoo.com  from=gmail.com; domainkeys=neutral (no sig);  from=gmail.com; dkim=pass (ok)
Received: from 127.0.0.1  (EHLO mail-we0-f172.google.com) (74.125.82.172)
  by mta1577.mail.ne1.yahoo.com with SMTP; Wed, 06 Nov 2013 18:16:33 +0000
Received: by mail-we0-f172.google.com with SMTP id q58so5392697wes.3
        for <test_account@yahoo.com>; Wed, 06 Nov 2013 10:16:32 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:date:message-id:subject:from:to:content-type;
        bh=dlBHSl/ACP7PJuXYWPaPhCBGdI26QbEp7CxORuaZ5BU=;
        b=BPGA7wege39PvP3flMtaevMxve1kb8xZUsocFOxhFBKDzlg0+MWjIvFnNNiDiG8EkU
         Y/l8AkRGl0Gp1OrNN7Kud65fdNvTgBySAySwjC/Hlet4bkWMv5VikRHj8QNPQ1nML2k/
         z8eF5LMQMXSIZ69DFzEDsTggJUkWRzgdTf9wgTJlpwffEvzir3R/hizcGTMInD0UzOeW
         q8f3Vm5sF2y+SenPXkTBzHmdS6Ugsq8x9qm0Uqx5qJbKxhx6xYpS5/sAfy/XgHmdGSar
         pvQMnF26f3hFvHUfbvj4gUQri1j/qrJbqJL19RjtcDnJKAU8AX2b98WGmIX+bjLlbjIV
         oP/Q==
MIME-Version: 1.0
X-Received: by 10.194.88.225 with SMTP id bj1mr2994653wjb.50.1383761792331;
```

Email Header Analysis: Gmail Email



```
Delivered-To: eb216071@gmail.com

Received: by 10.231.161.193 with SMTP id s1cs304470ibx; Mon, 6 Dec 2010 08:49:22 -0800 (PST)

Received: by 10.142.253.21 with SMTP id a21mr5387394wfi.219.1291654162218; Mon, 06 Dec 2010 08:49:22 -0800 (PST)

Return-Path: <mrobinsn@aol.com>

Received: from imr-da04.mx.aol.com (imr-da04.mx.aol.com [205.188.105.146]) by
 mx.google.com with ESMTP id m14si11167105qcu.74.2010.12.06.08.49.21; Mon, 06 Dec 2010 08:49:22 -0800 (PST)

Received-SPF: pass (google.com: domain of mrobinsn@aol.com designates 205.188.105.146 as permitted sender)
 client-ip=205.188.105.146;

Authentication-Results: mx.google.com; spf=pass (google.com: domain of mrobinsn@aol.com designates
205.188.105.146 as permitted sender)
 smtp.mail=mrobinsn@aol.com

Received: from mtaomg-mb03.r1000.mx.aol.com (mtaomg-mb03.r1000.mx.aol.com
 [172.29.41.74]) by imr-da04.mx.aol.com (8.14.1/8.14.1) with ESMTP id oB6GmxoP013794 for <eb216071@gmail.com>;
Mon, 6 Dec 2010 11:49:13 -0500

Received: from core-mkb001b.r1000.mail.aol.com (core-mkb001.r1000.mail.aol.com [172.29.98.1])
 by mtaomg-mb03.r1000.mx.aol.com (OMAG/Core Interface)
 with ESMTP id AFFCCE000086 for <eb216071@gmail.com>; Mon, 6 Dec 2010 11:49:13 -0500 (EST)

To: Eddie <eb216071@gmail.com>

Subject: hey sweetie

X-MB-Message-Source: WebUI
X-AOL-IP: 214.16.41.245
X-MB-Message-Type: User
MIME-Version: 1.0

From: Monica <mrobinsn@aol.com>

Content-Type: multipart/alternative;
 boundary="--------MB_8CD637CA59DCFBE_1CB4_7630_Webmail-d112.sysops.aol.com"
X-Mailer: AOL Webmail 32992-STANDARD

Received: from 214.16.41.245 by Webmail-d112.sysops.aol.com (205.188.171.229)
 with HTTP (WebMailUI); Mon, 06 Dec 2010 11:49:13 -0500

Message-Id: <8CD637CA59DCFBE-1CB4-2D92@Webmail-d112.sysops.aol.com>
X-Originating-IP: [214.16.41.245]

Date: Mon, 6 Dec 2010 11:49:13 -0500 (EST)

x-aol-global-disposition: G
X-AOL-SCOLL-SCORE: 0:2:308094592:93952408
X-AOL-SCOLL-URL_COUNT: 0
x-aol-sid: 3039ac1d294a4cfd14094e2f
```

SPF, DKIM & DMARC Mechanisms

- For dealing with email spoofing & validating email authenticity:
  - **Sender Policy Framework (SPF)**
  - **DomainKeys Identified Mail (DKIM)**
  - **Domain-based Message Authentication, Reporting and Conformance (DMARC)**
- **References** (good videos):
  - SPF, DKIM & DMARC mechanisms: https://www.youtube.com/watch?v=KJM8IdP27cQ
  - Forensic analysis (including on various timestamps recorded): https://www.youtube.com/watch?v=nK5QpGSBR8c

Sender Policy Framework (SPF)

- SMTP permits ***any* computer** to send email claiming to be from ***any* source address** → various following issues:
  - **Forged email addresses**: by spammers & scammers
  - Also used in **phishing techniques**: an email purportedly sent by a bank, etc.
  - **Email tracing** back to its source is thus more difficult
- **SPF**:
  - Allows a domain owner to specify which computers **are authorized to send mail** with envelope-from addresses **in that domain**
  - Uses **DNS TXT records**
  - Receivers verifying the **SPF information** in DNS TXT records may reject messages from unauthorized sources
- Reference: https://en.wikipedia.org/wiki/Sender_Policy_Framework

DomainKeys Identified Mail (DKIM)

- DKIM allows the email receiver to check that an email was indeed **authorized** by the owner of that domain
- It affixes a ***digital signature***, linked to a domain name, to each outgoing email message
- The recipient system can verify this by looking up the **sender's *public key*** published in the DNS record
- A valid signature guarantees that some parts of the email (possibly including attachments) **have not been modified**
- Reference: https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail

Domain-based Message Authentication, *Reporting and Conformance* (DMARC)

- **DMARC** extends SPF and DKIM: to allow the administrative owner of a domain to publish a **policy** that specifies:
  - Which **mechanism** (DKIM, SPF or both) is employed when sending email from that domain
  - How the receiver should deal with ***failures***
  - A ***reporting mechanism*** for actions performed under those policies
- A receiving email server authenticates the incoming email based on the instructions in the **DNS DMARC entry**:
  - If the email passes the authentication: it will be delivered & can be trusted
  - If the email **fails** the check: depending on the instructions in the DMARC record, the email could be **delivered, quarantined or rejected**
- Reference: https://en.wikipedia.org/wiki/DMARC

MS Outlook: PST File & Its Analysis

- ***MS Outlook data*** **(*PST*)** file:
  - Contains **messages** and other **Outlook items** saved on user computer
  - Used by certain types of accounts, such as POP accounts
- **Locations**:
  - Windows 7: C:\Users\%username%\My Documents\Outlook Files
  - Windows 8+: C:\Users\%username%\Documents\Outlook Files
- PST **file structure**:
  - https://www.mailxaminer.com/blog/outlook-2013-email-forensics/
- Forensics **tools**:
  - Various **PST readers**, including **readpst** (https://linux.die.net/man/1/readpst)

MS Outlook: Other File & Folder

- ***Offline Outlook data* (*OST*)** file
  - Used by account like **IMAP** accounts, **Office 365** accounts, **Exchange** accounts, and **Outlook.com** accounts
  - Stores a ***synchronized copy*** of mailbox information on the user's local computer
  - When user connection to the mail server is **interrupted**, the user you can still access all emails, calendar data, contacts that have been previously downloaded
- Ref: https://support.office.com/en-us/article/introduction-to-outlook-data-files-pst-and-ost-222eaf92-a995-45d9-bde2-f331f60e2790

- Outlook temporary **OLK folder**: http://www.hancockcomputertech.com/blog/2010/01/06/find-the-microsoft-outlook-temporary-olk-folder/

Other Internet Artefacts: *Skype History*

- Keeps a log of ***chat sessions*** and files transferred from one machine to another
- Is **turned on** by default in Skype installations
- **Locations**:
  - XP: C:\Documents and Settings\<*username*>\Application\Skype\<*skype-name*>
  - Win7/8/10: C:\%USERPROFILE%\AppData\Roaming\Skype\<*skype-name*>

Lab 7 Exercises

- Task 1: Finding out **network configuration settings** of a target Windows machine
- *(Optional)* Task 2: Analyzing captured **network-traffic logs** using Wireshark
- Task 3: Analyzing captured **network-traffic logs** and **data/objects contained** using NetworkMiner & (*optional*) Xplico
- Task 4: Extracting and analyzing **web cache** & **history**

- ***Graded Lab Tasks #4*: 2 weeks are given** (due to the mid-term test next week)

Offline Discussion: For Your Own Review

- Give an example of **the type of digital evidence** that can be found at ***each of OSI network layers***, and how it can be **useful** to a forensic investigation!

- What are ***some possible difficulties*** in relying on an observed **IP address** or a **MAC address**? How would you overcome these difficulties?

Questions?

See you next week

(with the mid-term exam)!