Topic 2 Evidence in computers and networks Part 3

Learning Outcome

- After successfully completing this lecture, you will be able to
  - Describe evidence in networks
    - Network Traffic
    - Social Media
  - Describe and apply techniques and technologies in acquisition and duplication of evidence data from network traffic and social media

Road Map

- Network Traffic Data
- Social Media Data

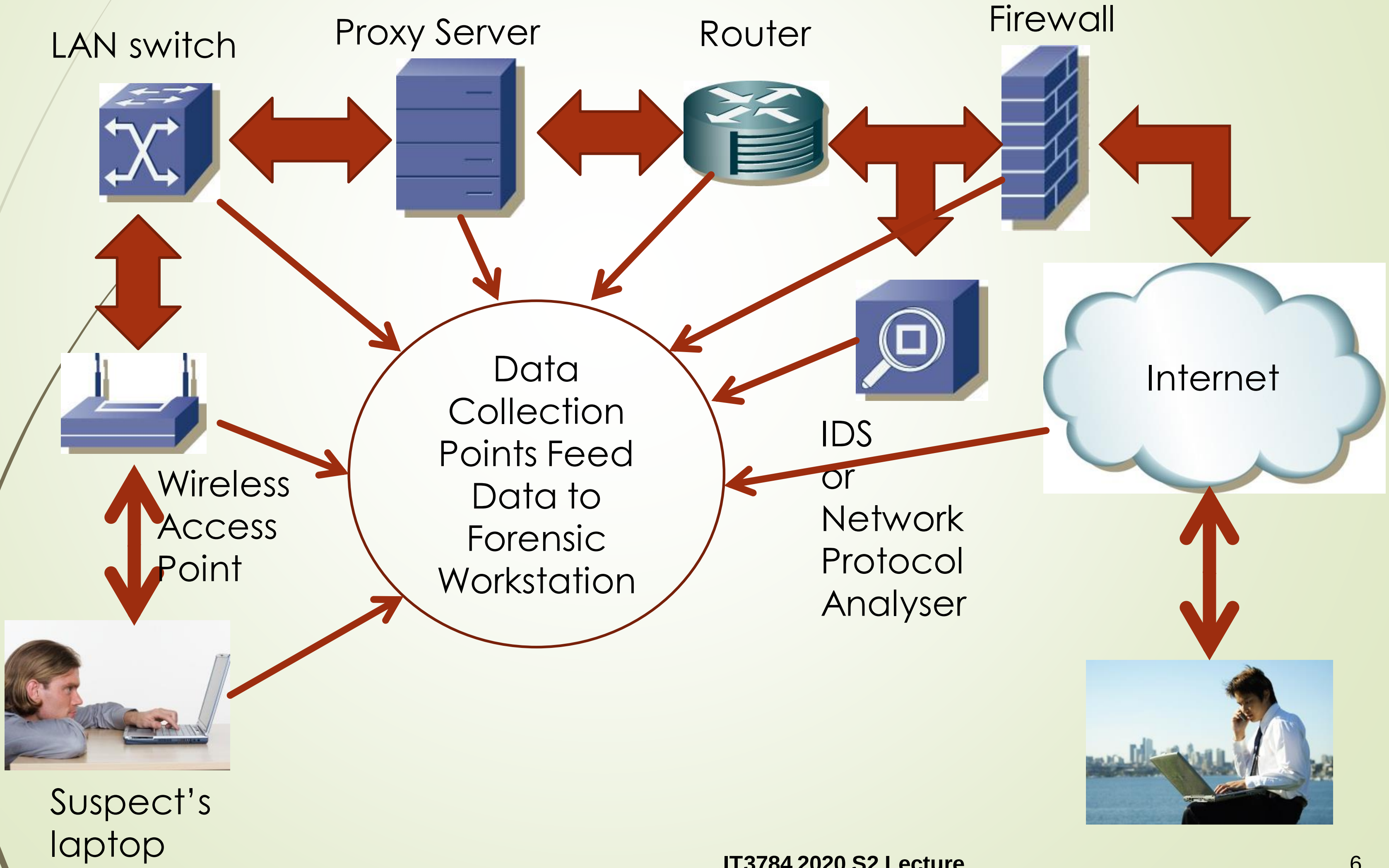
How can you do it?

- It was reported that an employee used online chat at his laptop to disclose the secret recipe of a company product to a person who is working for the competitor.
- The employee later set fire on his laptop and data cannot be acquired from the laptop.
- You are asked to acquire evidence data related to this case.

Data Acquisition and Duplication

- Identify possible sources of data
  - Network traffic
  - Online chat - social media
- Develop a plan to acquire the data
  - Likely Value – The network traffic and online chat contains the disclosed secret recipe
  - Volatility – Network traffic is volatile but messages in social media is not
  - Amount of Effort Required – Physical acquisition of network traffic and logical acquisition of social media data
- Acquire the data
  - How to do it?
- Verify the integrity of the data
  - Hash values required

Network Data Collection Points

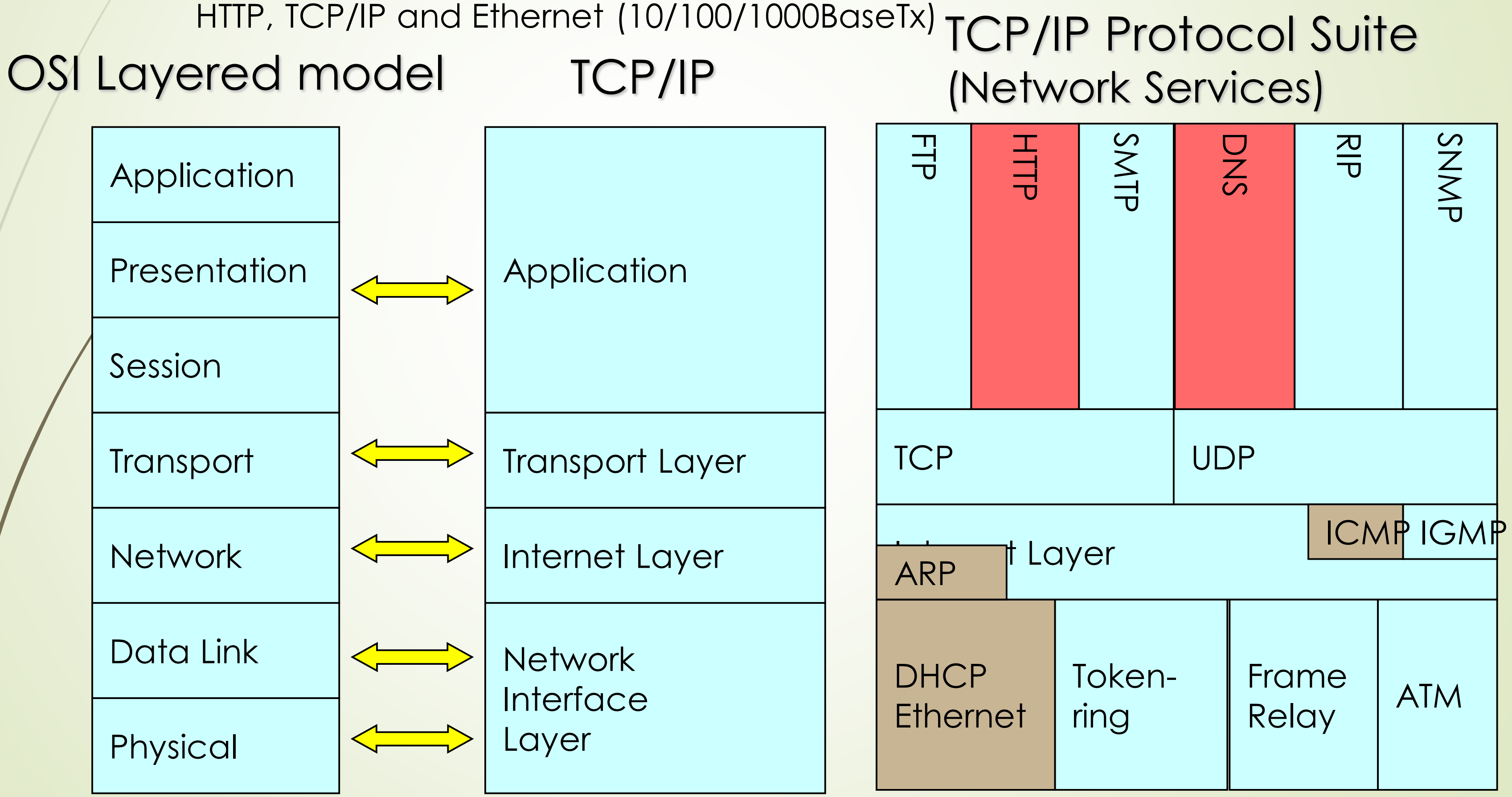

LAN switch
Proxy Server
Router
Firewall
Internet
Wireless Access Point
Data Collection Points Feed Data to Forensic Workstation
IDS or Network Protocol Analyser
Suspect's laptop

Where can we capture network traffic?

- Warning: You must obtain the permission from the owner of the network BEFORE collection of data packets from the network.
- Run a network monitoring or a network protocol analyser tool such as Wireshark, tcpdump
  - At the end point, a network server such as proxy server to collect
    - Broadcast traffic, such as ARP and BROWSER, and
    - Unicast traffic sent and received at the end point
  - At a forensic PC connected to the mirror port of a Internet Router, to collect
    - Unicast traffic between computers in the untrusted Internet and the computers in the trusted intranet

Network Services Protocols

HTTP, TCP/IP and Ethernet (10/100/1000BaseTx)



OSI Layered model

Application

Presentation

Session

Transport

Network

Data Link

Physical

TCP/IP

Application

Transport Layer

Internet Layer

Network Interface Layer

TCP/IP Protocol Suite (Network Services)

FTP

HTTP

SMTP

DNS

RIP

SNMP

TCP

UDP

t Layer

ARP

ICMP IGMP

DHCP Ethernet

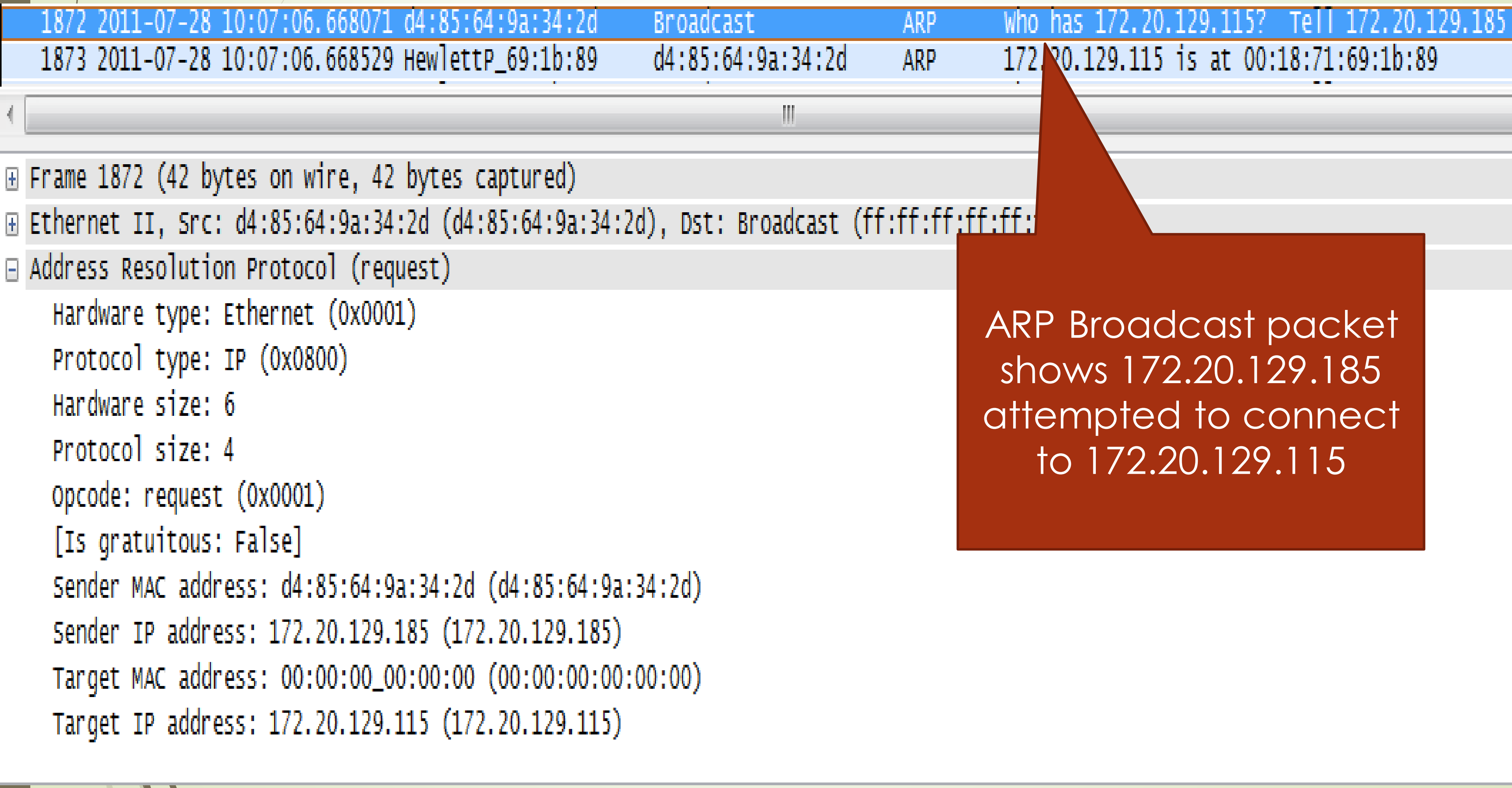
Token-ring

Frame Relay

ATM

Find list of TCP UDP and IP network services in c:\Windows\System32\drivers\etc\services

Address Resolution Protocol Broadcast Traffic

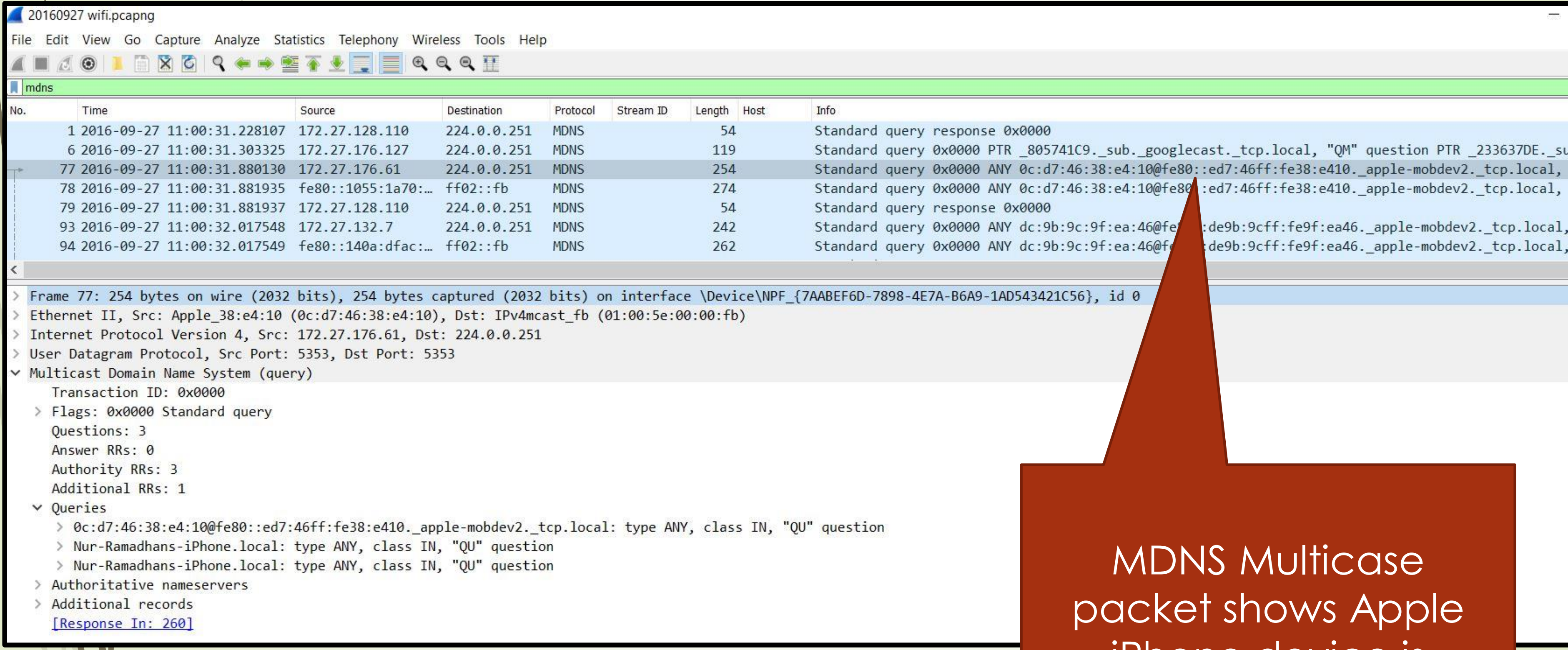


```
1872 2011-07-28 10:07:06.668071 d4:85:64:9a:34:2d    Broadcast          ARP    Who has 172.20.129.115?  Tell 172.20.129.185
1873 2011-07-28 10:07:06.668529 HewlettP_69:1b:89    d4:85:64:9a:34:2d  ARP    172.20.129.115 is at 00:18:71:69:1b:89
```

```
⊞ Frame 1872 (42 bytes on wire, 42 bytes captured)
⊞ Ethernet II, Src: d4:85:64:9a:34:2d (d4:85:64:9a:34:2d), Dst: Broadcast (ff:ff:ff:ff:ff:
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    [Is gratuitous: False]
    Sender MAC address: d4:85:64:9a:34:2d (d4:85:64:9a:34:2d)
    Sender IP address: 172.20.129.185 (172.20.129.185)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.20.129.115 (172.20.129.115)
```

ARP Broadcast packet shows 172.20.129.185 attempted to connect to 172.20.129.115

MDNS Multicase DNS packets show brands and types of network devices in the network



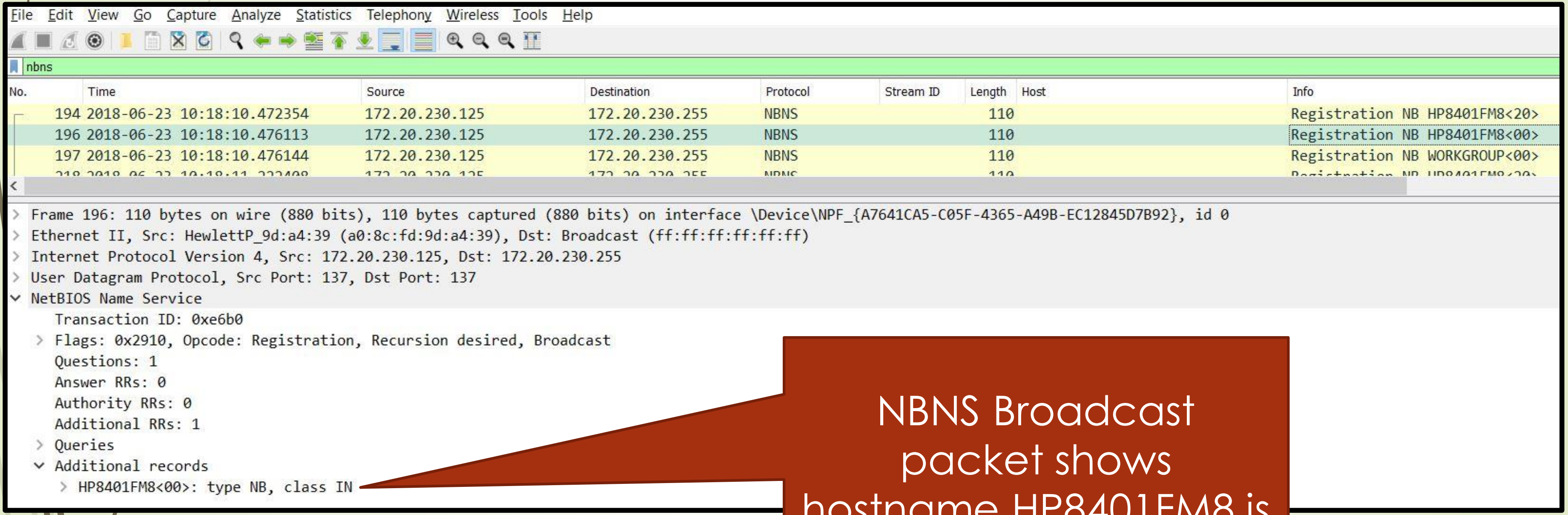
20160927 wifi.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
mdns

```
No.   Time                        Source             Destination   Protocol  Stream ID  Length  Host  Info
    1 2016-09-27 11:00:31.228107  172.27.128.110     224.0.0.251   MDNS                     54        Standard query response 0x0000
    6 2016-09-27 11:00:31.303325  172.27.176.127     224.0.0.251   MDNS                    119        Standard query 0x0000 PTR _805741C9._sub._googlecast._tcp.local, "QM" question PTR _233637DE._su
   77 2016-09-27 11:00:31.880130  172.27.176.61      224.0.0.251   MDNS                    254        Standard query 0x0000 ANY 0c:d7:46:38:e4:10@fe80::ed7:46ff:fe38:e410._apple-mobdev2._tcp.local,
   78 2016-09-27 11:00:31.881935  fe80::1055:1a70:…  ff02::fb      MDNS                    274        Standard query 0x0000 ANY 0c:d7:46:38:e4:10@fe80 :ed7:46ff:fe38:e410._apple-mobdev2._tcp.local,
   79 2016-09-27 11:00:31.881937  172.27.128.110     224.0.0.251   MDNS                     54        Standard query response 0x0000
   93 2016-09-27 11:00:32.017548  172.27.132.7       224.0.0.251   MDNS                    242        Standard query 0x0000 ANY dc:9b:9c:9f:ea:46@fe  :de9b:9cff:fe9f:ea46._apple-mobdev2._tcp.local,
   94 2016-09-27 11:00:32.017549  fe80::140a:dfac:…  ff02::fb      MDNS                    262        Standard query 0x0000 ANY dc:9b:9c:9f:ea:46@f  :de9b:9cff:fe9f:ea46._apple-mobdev2._tcp.local,
```

```
> Frame 77: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF_{7AABEF6D-7898-4E7A-B6A9-1AD543421C56}, id 0
> Ethernet II, Src: Apple_38:e4:10 (0c:d7:46:38:e4:10), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 172.27.176.61, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
v Multicast Domain Name System (query)
    Transaction ID: 0x0000
  > Flags: 0x0000 Standard query
    Questions: 3
    Answer RRs: 0
    Authority RRs: 3
    Additional RRs: 1
  v Queries
    > 0c:d7:46:38:e4:10@fe80::ed7:46ff:fe38:e410._apple-mobdev2._tcp.local: type ANY, class IN, "QU" question
    > Nur-Ramadhans-iPhone.local: type ANY, class IN, "QU" question
    > Nur-Ramadhans-iPhone.local: type ANY, class IN, "QU" question
  > Authoritative nameservers
  > Additional records
    [Response In: 260]
```

MDNS Multicase packet shows Apple iPhone device is present in the network

NBNS Broadcast packets show brands and types of network devices in the network


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

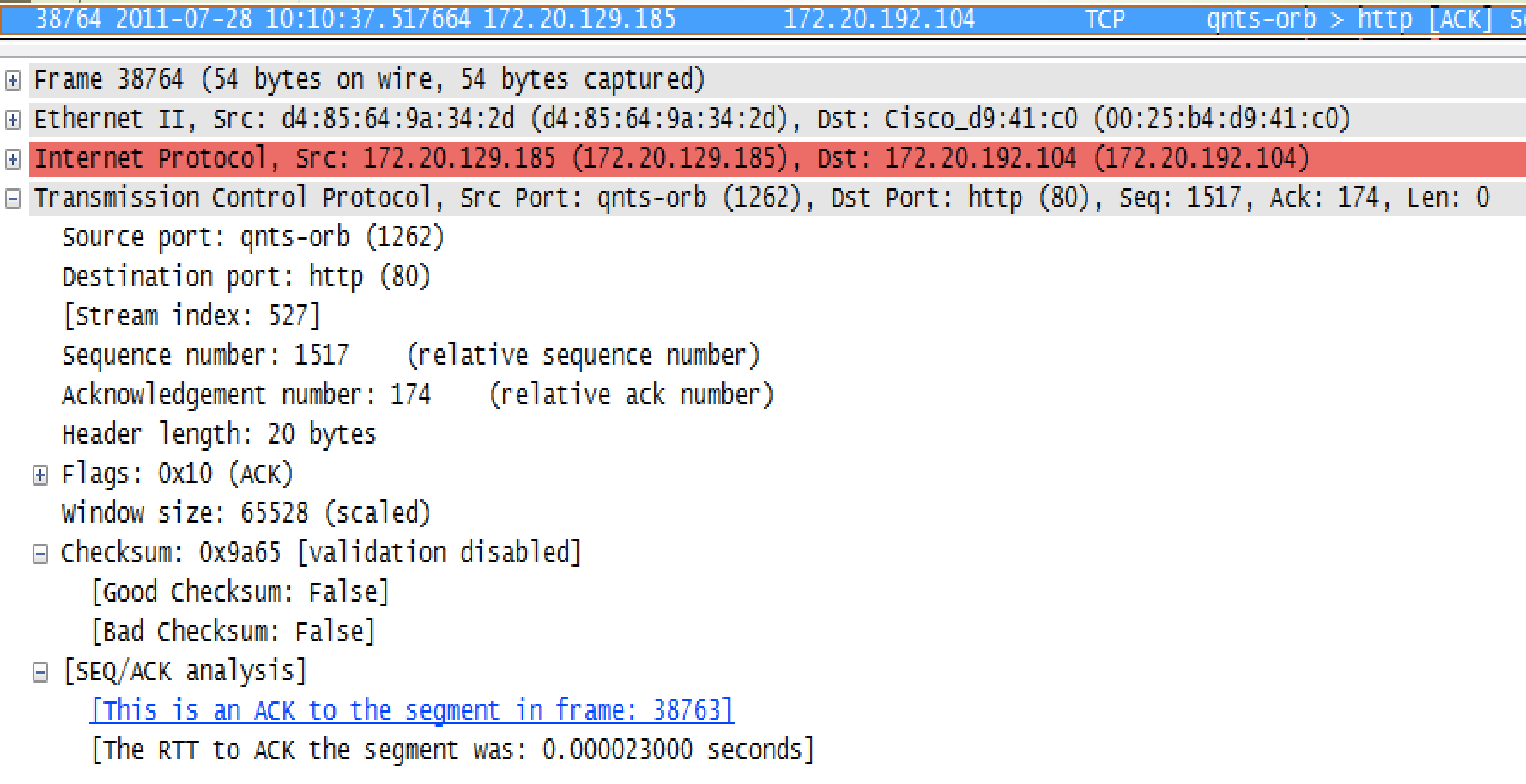
nbns

```
No.   Time                        Source            Destination       Protocol  Stream ID  Length  Host  Info
  194 2018-06-23 10:18:10.472354  172.20.230.125    172.20.230.255    NBNS                    110        Registration NB HP8401FM8<20>
  196 2018-06-23 10:18:10.476113  172.20.230.125    172.20.230.255    NBNS                    110        Registration NB HP8401FM8<00>
  197 2018-06-23 10:18:10.476144  172.20.230.125    172.20.230.255    NBNS                    110        Registration NB WORKGROUP<00>
  218 2018-06-23 10:18:11.222408  172.20.230.125    172.20.230.255    NBNS                    110        Registration NB HP8401FM8<20>
```

```
> Frame 196: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{A7641CA5-C05F-4365-A49B-EC12845D7B92}, id 0
> Ethernet II, Src: HewlettP_9d:a4:39 (a0:8c:fd:9d:a4:39), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.20.230.125, Dst: 172.20.230.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
v NetBIOS Name Service
    Transaction ID: 0xe6b0
  > Flags: 0x2910, Opcode: Registration, Recursion desired, Broadcast
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  > Queries
  v Additional records
    > HP8401FM8<00>: type NB, class IN
```

NBNS Broadcast packet shows hostname HP8401FM8 is registering itself to the NetBIOS name server

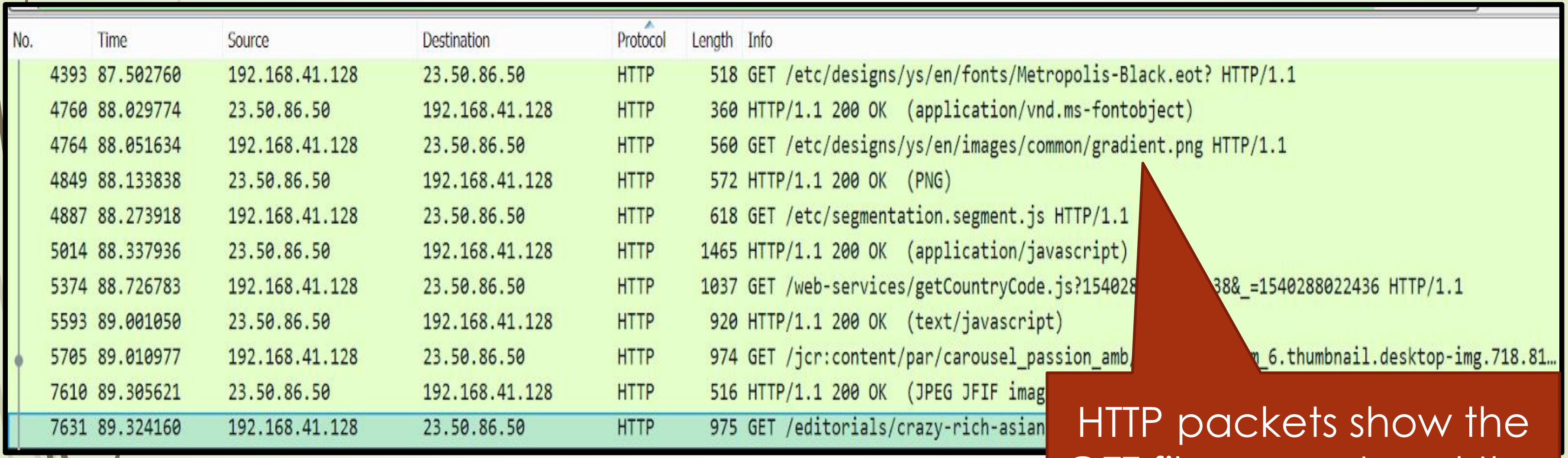
HTTP Protocol Unicast Traffic



```
38764 2011-07-28 10:10:37.517664 172.20.129.185        172.20.192.104        TCP      qnts-orb > http [ACK] S

⊞ Frame 38764 (54 bytes on wire, 54 bytes captured)
⊞ Ethernet II, Src: d4:85:64:9a:34:2d (d4:85:64:9a:34:2d), Dst: Cisco_d9:41:c0 (00:25:b4:d9:41:c0)
⊞ Internet Protocol, Src: 172.20.129.185 (172.20.129.185), Dst: 172.20.192.104 (172.20.192.104)
⊟ Transmission Control Protocol, Src Port: qnts-orb (1262), Dst Port: http (80), Seq: 1517, Ack: 174, Len: 0
    Source port: qnts-orb (1262)
    Destination port: http (80)
    [Stream index: 527]
    Sequence number: 1517    (relative sequence number)
    Acknowledgement number: 174    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size: 65528 (scaled)
  ⊟ Checksum: 0x9a65 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
  ⊟ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 38763]
      [The RTT to ACK the segment was: 0.000023000 seconds]
```

13

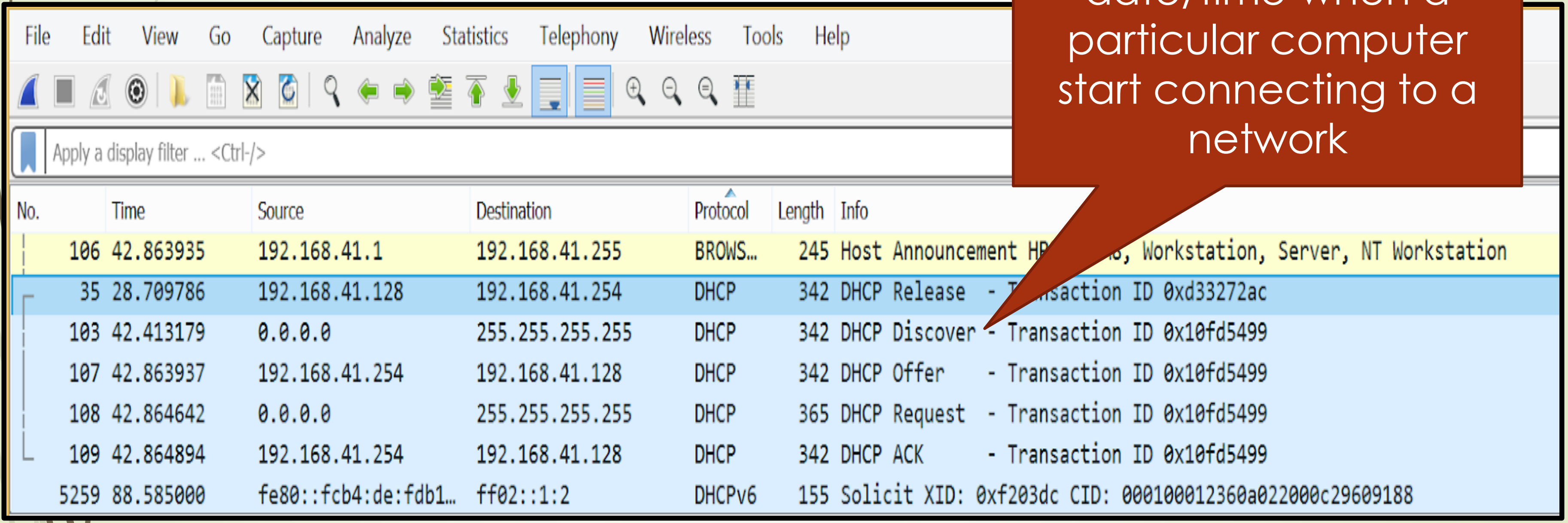
HTTP Unicast packets contain URL attack strings and file transferred between the web server and the client



No.	Time	Source	Destination	Protocol	Length	Info
4393	87.502760	192.168.41.128	23.50.86.50	HTTP	518	GET /etc/designs/ys/en/fonts/Metropolis-Black.eot? HTTP/1.1
4760	88.029774	23.50.86.50	192.168.41.128	HTTP	360	HTTP/1.1 200 OK (application/vnd.ms-fontobject)
4764	88.051634	192.168.41.128	23.50.86.50	HTTP	560	GET /etc/designs/ys/en/images/common/gradient.png HTTP/1.1
4849	88.133838	23.50.86.50	192.168.41.128	HTTP	572	HTTP/1.1 200 OK (PNG)
4887	88.273918	192.168.41.128	23.50.86.50	HTTP	618	GET /etc/segmentation.segment.js HTTP/1.1
5014	88.337936	23.50.86.50	192.168.41.128	HTTP	1465	HTTP/1.1 200 OK (application/javascript)
5374	88.726783	192.168.41.128	23.50.86.50	HTTP	1037	GET /web-services/getCountryCode.js?154028 38&_=1540288022436 HTTP/1.1
5593	89.001050	23.50.86.50	192.168.41.128	HTTP	920	HTTP/1.1 200 OK (text/javascript)
5705	89.010977	192.168.41.128	23.50.86.50	HTTP	974	GET /jcr:content/par/carousel_passion_amb m_6.thumbnail.desktop-img.718.81…
7610	89.305621	23.50.86.50	192.168.41.128	HTTP	516	HTTP/1.1 200 OK (JPEG JFIF imag
7631	89.324160	192.168.41.128	23.50.86.50	HTTP	975	GET /editorials/crazy-rich-asian

HTTP packets show the GET file request and the successful transfer of files and data between the web server and the client

DHCP protocol that generate both broadcast and unicast traffic

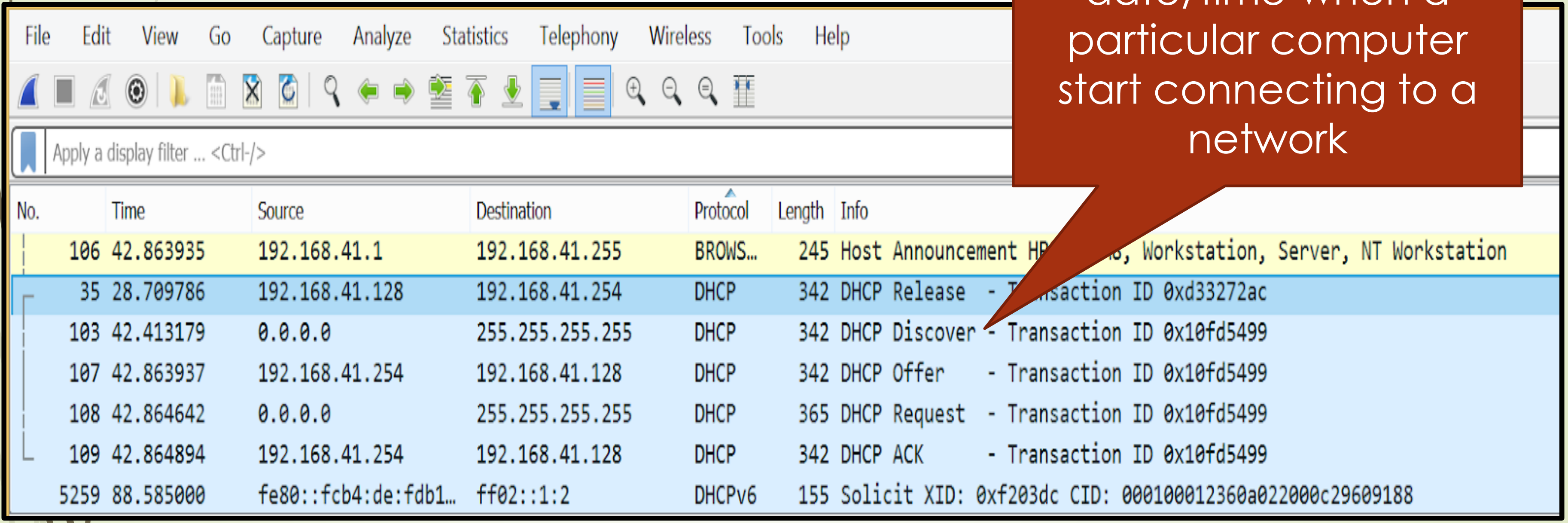


No.	Time	Source	Destination	Protocol	Length	Info
106	42.863935	192.168.41.1	192.168.41.255	BROWS…	245	Host Announcement HP s, Workstation, Server, NT Workstation
35	28.709786	192.168.41.128	192.168.41.254	DHCP	342	DHCP Release - T nsaction ID 0xd33272ac
103	42.413179	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x10fd5499
107	42.863937	192.168.41.254	192.168.41.128	DHCP	342	DHCP Offer - Transaction ID 0x10fd5499
108	42.864642	0.0.0.0	255.255.255.255	DHCP	365	DHCP Request - Transaction ID 0x10fd5499
109	42.864894	192.168.41.254	192.168.41.128	DHCP	342	DHCP ACK - Transaction ID 0x10fd5499
5259	88.585000	fe80::fcb4:de:fdb1…	ff02::1:2	DHCPv6	155	Solicit XID: 0xf203dc CID: 000100012360a022000c29609188

DHCP Discover Packet give the evidence on date/time when a particular computer start connecting to a network

DHCP protocol that generate both broadcast and unicast traffic

DHCP Discover Packet give the evidence on date/time when a particular computer start connecting to a network



```
No.   Time       Source            Destination      Protocol  Length Info
 106  42.863935  192.168.41.1      192.168.41.255   BROWS...   245 Host Announcement HP[illegible], Workstation, Server, NT Workstation
  35  28.709786  192.168.41.128    192.168.41.254   DHCP       342 DHCP Release  - Transaction ID 0xd33272ac
 103  42.413179  0.0.0.0           255.255.255.255  DHCP       342 DHCP Discover - Transaction ID 0x10fd5499
 107  42.863937  192.168.41.254    192.168.41.128   DHCP       342 DHCP Offer    - Transaction ID 0x10fd5499
 108  42.864642  0.0.0.0           255.255.255.255  DHCP       365 DHCP Request  - Transaction ID 0x10fd5499
 109  42.864894  192.168.41.254    192.168.41.128   DHCP       342 DHCP ACK      - Transaction ID 0x10fd5499
5259  88.585000  fe80::fcb4:de:fdb1… ff02::1:2      DHCPv6     155 Solicit XID: 0xf203dc CID: 000100012360a022000c29609188
```

Network Data Acquisition Evidence in Different Layers

- Application
  - This layer sends and receives data for particular applications, such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).
- Transport
  - This layer provides connection-oriented or connectionless services for transporting application layer services between networks. The transport layer can optionally ensure the reliability of communications. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are commonly used transport layer protocols.

Network Data Acquisition Evidence in Different Layers

- Network
  - This layer routes packets across networks. IP is the fundamental network layer protocol for TCP/IP. Other commonly used protocols at the network layer are Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP).
- Data Link
  - This layer handles communications on the physical network components. The best known data link layer protocol is Ethernet.

Network Traffic Forensics

- Network forensic analysis relies on all of the layers.

1. When analysts begin to examine data, they typically have limited information□most likely an IP address of interest and perhaps protocol and port information. This is enough information to support searching common data sources for more information.
2. In most cases, the application layer contains the actual activity of interest□Most attacks are against vulnerabilities in applications, and nearly all misuse involves misuse of applications.
3. Analysts need IP addresses so that they can identify the hosts that may have been involved in the activity. The hosts may also contain additional data that would be of use in analyzing the activity.
4. Some events of interest may not have relevant application-level data (e.g., a distributed denial of service attack designed to consume all network bandwidth), most do; network forensics provides important support to the analysis of application-layer activities.

Network Routers

- Evidence in Network Routers
  - Routing table
  - Access Control List (ACL)
  - Blocked incoming/outgoing packets (not meeting ACL rules)
  - Error logs
  - Optional information
    - Packets forwarded
    - Routing information shared with other routers

Network LAN Switches

- Evidence in Network Switches
  - MAC addresses of computers connected at each switch port
  - Date and time each MAC address was last detected at a particular port
  - IP addresses of computers connected at each port
  - Hostnames of computers connected at each port
  - History logs on blocked broadcast traffic
  - Error logs

Network Firewalls

- Evidence in Firewalls Switches
  - Firewalls Rules
    - TCP/IP filtering rules
    - Users, application restriction rules
    - User groups and their security policies
  - Blocked incoming and outgoing network traffic
    - Most firewalls send event logs to a network log server for archive purpose.

Network Proxy Servers

- Evidence in Proxy Servers
  - Internet browsing history of each user and computer in the company intranet
  - Black-listed websites
  - Decrypted SSL connection application data between the attackers' computers in Internet and the victim computers in the company Intranet.

Social Media Forensics

- Social Media
  - Facebook
  - Twitter
  - Gmail, Goolge+
  - LinkedIn
  - Gmail
  - YouTube

Data Acquisition and Duplication

- Evidence can be collected from information that is available in public
  - Unethical to create a fake account for the purpose of accessing someone’s information
- Information can be commonly found during the process of a computer or cell phone examination
  - In Internet history and unallocated space
  - Username or an email address can be used to find information about a person online
- Getting information from the service provider
  - Requires a criminal subpoena
  - Foreign Intelligence Surveillance Act, US
    - Google, Microsoft, Facebook, Twitter and Apple revealed US surveillance requests
  - Facebook Global Government Request Report
    - Singapore government: 107 requests on 117 individuals pertaining to criminal cases

Data Acquisition and Duplication

- Acquisition Challenges
  - Most artifacts are stored in websites
  - Require forensic examiners to develop applications to capture
  - Websites provide limited logical acquisition via Application Program Interface (API)

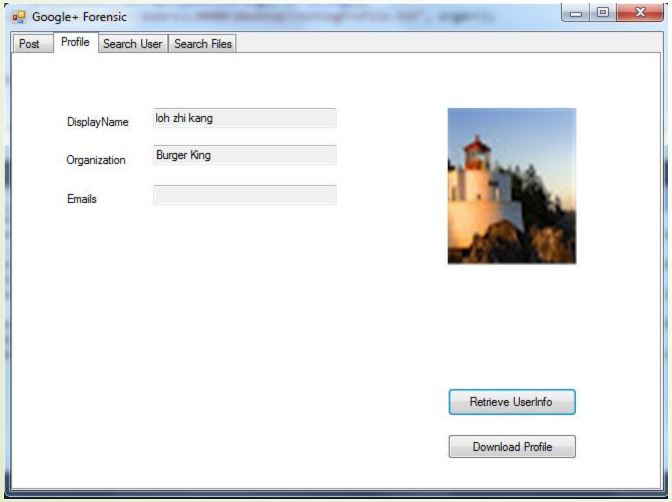
26

Oauth 2.0 Protocol

- Oauth2.0 (RFC6749) allows users to share their private resources such as contact lists and photos stored on one site, say flickr, with another site, say Facebook, without having to handout their credentials.
- Examiners use it to get their data acquisition applications authenticated to social media websites and get authorization on acquiring users' data
- Learn the basic Oauth 2.0 from the youtube video "OAuth 2.0 : An Overview"

Google+ Profile

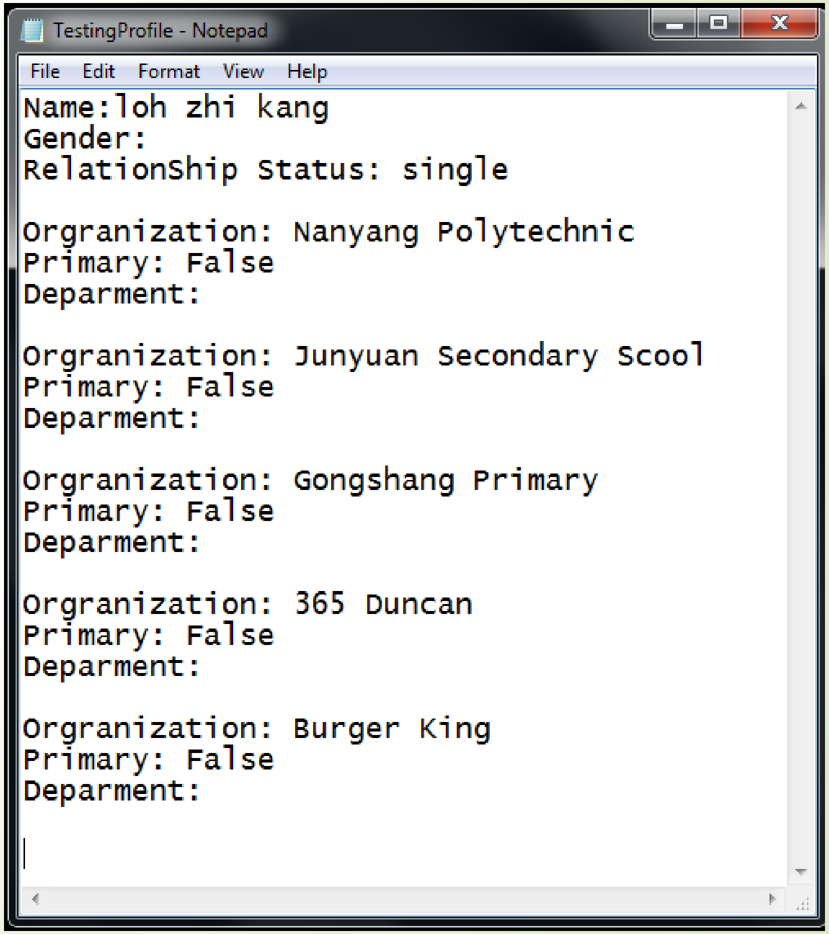
- Retrieve User profile
  - Name
  - Organization
  - UserID
  - Image



DisplayName: loh zhi kang

Organization: Burger King

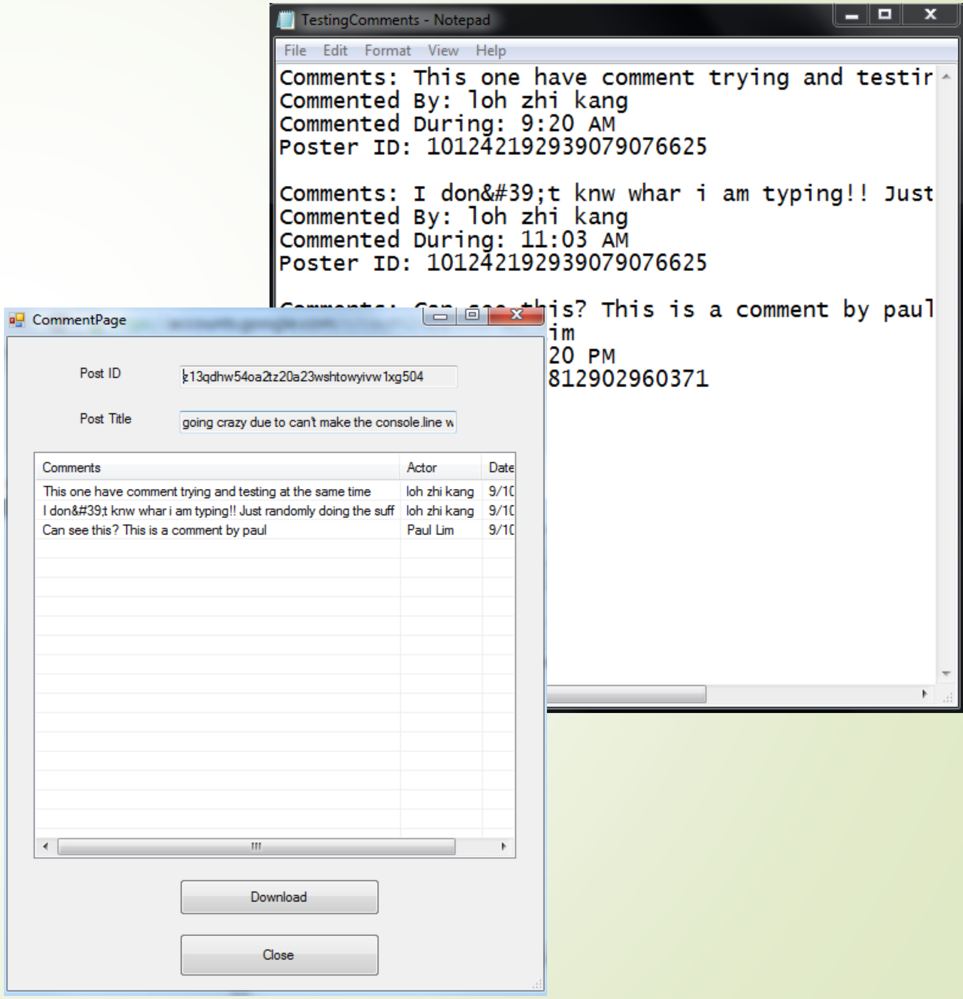
Emails:



```
Name:loh zhi kang
Gender:
RelationShip Status: single

Orgranization: Nanyang Polytechnic
Primary: False
Deparment:

Orgranization: Junyuan Secondary Scool
Primary: False
Deparment:

Orgranization: Gongshang Primary
Primary: False
Deparment:

Orgranization: 365 Duncan
Primary: False
Deparment:

Orgranization: Burger King
Primary: False
Deparment:
```

Google+ Comments

- Retrieved Comments
  - Comment Content
  - Commenter
  - Comment date
  - Post title
  - Post ID
  - Commenter ID



```
Comments: This one have comment trying and testir
Commented By: loh zhi kang
Commented During: 9:20 AM
Poster ID: 101242192939079076625

Comments: I don&#39;t knw whar i am typing!! Just
Commented By: loh zhi kang
Commented During: 11:03 AM
Poster ID: 101242192939079076625

Comments: Can see this? This is a comment by paul
                        im
                        20 PM
                        812902960371
```

Post ID: z13qdhw54oa2tz20a23wshtowyivw1xg504

Post Title: going crazy due to can't make the console.line w

Comments	Actor	Date
This one have comment trying and testing at the same time	loh zhi kang	9/10
I don&#39;t knw whar i am typing!! Just randomly doing the suff	loh zhi kang	9/10
Can see this? This is a comment by paul	Paul Lim	9/10

Facebook

- Facebook APIs provide logical acquisition of
  - Profile
  - Profile feed
  - Status
  - Friend list
  - News feed
  - Message Inbox
  - Photos
  - Check-ins

30

Gmail

- Google APIs can acquire
  - Messages in mail box
  - Calendar appointments
  - Google documents and spreadsheet
  - Photos
  - Blogs

Twitter

- Twitter APIs can logically acquire
  - Account details
  - Home timeline
  - User’s tweets
  - Tweets re-tweeted by
  - Tweets where the user is mentioned
  - Direct message to and from the user
  - Search tweet
  - Search for a user

Summary

- Network Traffic Data
  - Data Collection Points
  - Artifacts in 4 Different Layers
- Social Media Data
  - Limited Logical Acquisition
  - Oauth Protocol