Mag. iur. Dr. techn. Michael Sonntag

Collecting information

Institute for Information Processing and
Microprocessor Technology (FIM)
Johannes Kepler University Linz, Austria

E-Mail: sonntag@fim.uni-linz.ac.at
http://www.fim.uni-linz.ac.at/staff/sonntag.htm

Agenda

- NMap
- Web caches
- Web Archive
- WhoIs
- MX-Records
- Wireshark

NMap

- NMap (Network MAPper) is a network scanner
  - → It tries to find all computers in a specific network and checks what ports are open, what OS they are running, whether there is a firewall, etc.
- It does not look for specific vulnerabilities!
  - → But it gives recommendations; e.g. services to disable
  - → Some scans + vuln. systems → Lock-up/crash!
- Used as a tool for inventory generation in a network
  - → Are there any computers which should not be there?
  - → Can also be used to gather information for a later attack
    - » Which OS/software and which version is running
- Stages: 1 = Host discovery, 2 = Port scan, 3 = Service/ version detection, 4 = OS detection, 5 = Scripting
  - → Scripting may also include vulnerability/malware detection!

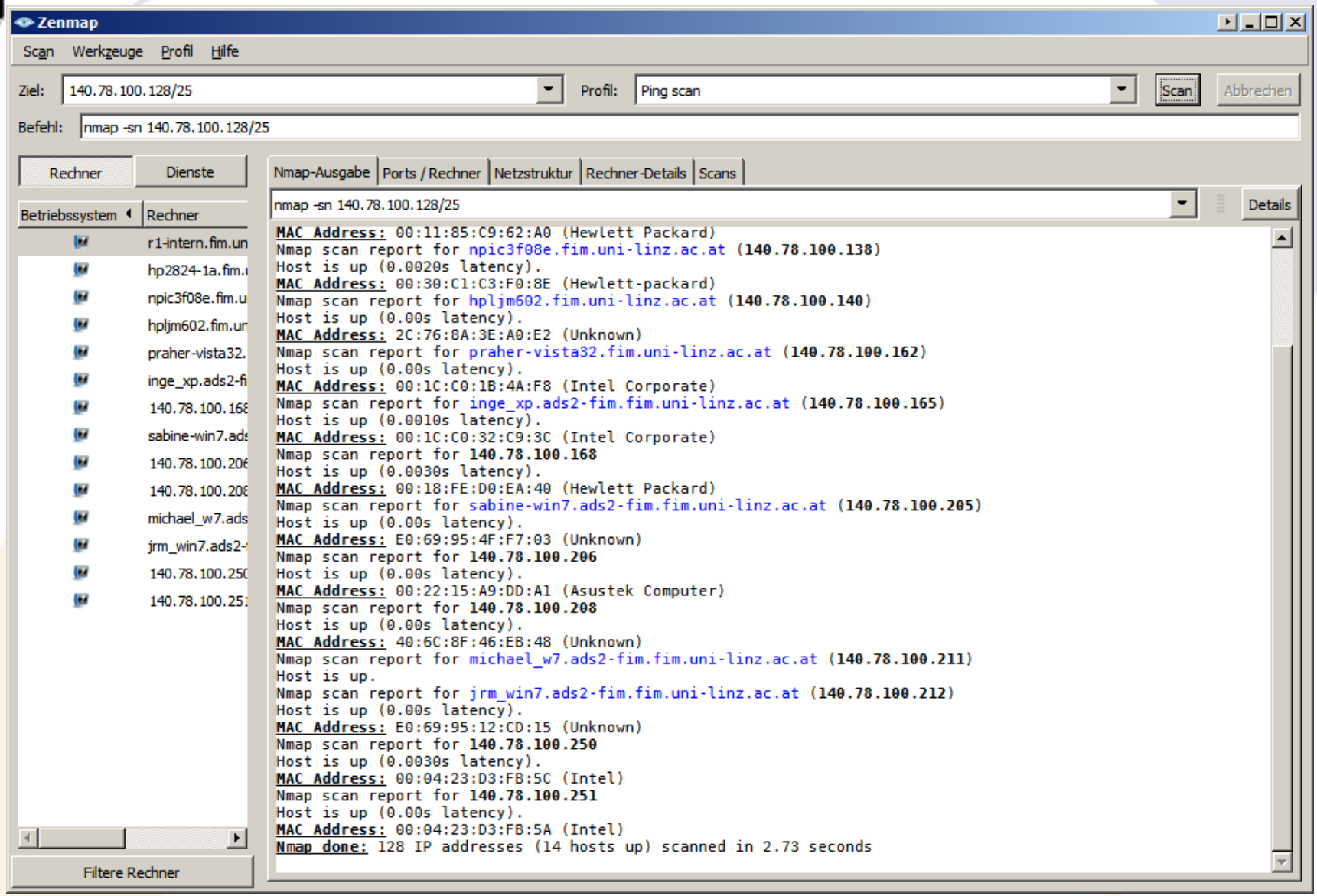
NMap and forensics

- To gather an “inventory” of what exists
  - → Computers → Try to find them physically, if they show up!
  - → Services → If port 22 is open, but no SSH server is running, you should investigate the computer in detail
    - » Hint at a rootkit, which hides itself
    - » Similar for “normal” and “public” services:
      - – Should they be running?
      - – What are they doing?
- Advantage: Happens from outside & from a trusted computer
  - → If the port is open, this cannot be hidden as e.g. from netstat!
- Where to find information on ports?
  - → C:\Windows\System32\drivers\etc\services
    - » Name, TCP, and/or UDP; sometimes a comment
  - → Google for the “unofficial” uses
  - → Official: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml
  - → See also: http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

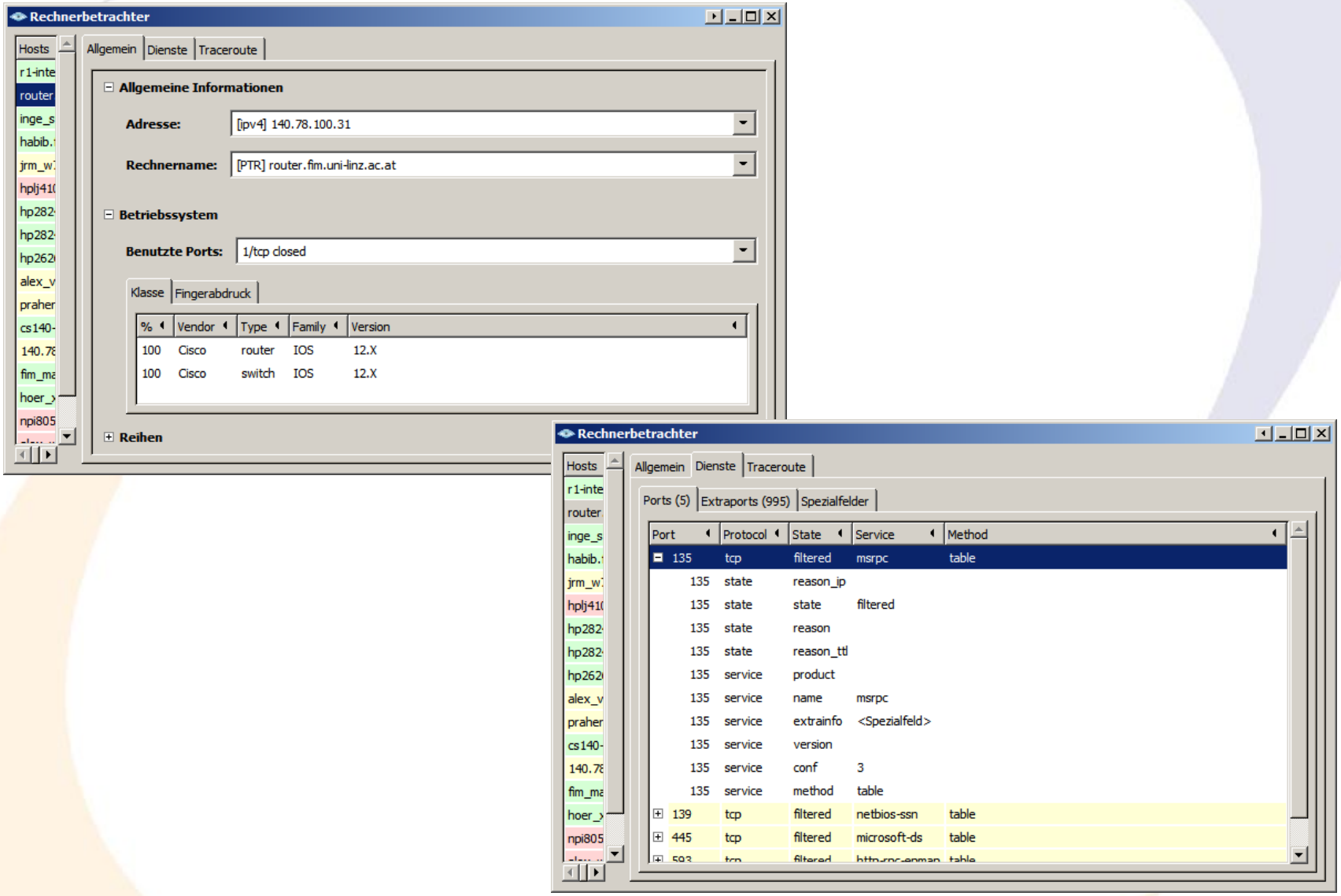
NMap

- Usage:
  - → Start program and enter IP address
  - → Select profile for scanning
    - » Special options only available in the command line version or when constructing a new profile!
- Your tasks:
  - → Install NMap (+ the UI – Zenmap)
  - → Scan the local subnet for hosts
    - » Use a “Quick scan"
  - → Scan the machine of your neighbour
    - » Use a “Regular scan"
  - → Interpret the results
    - » Correct output?
    - » Something surprising/dangerous found?

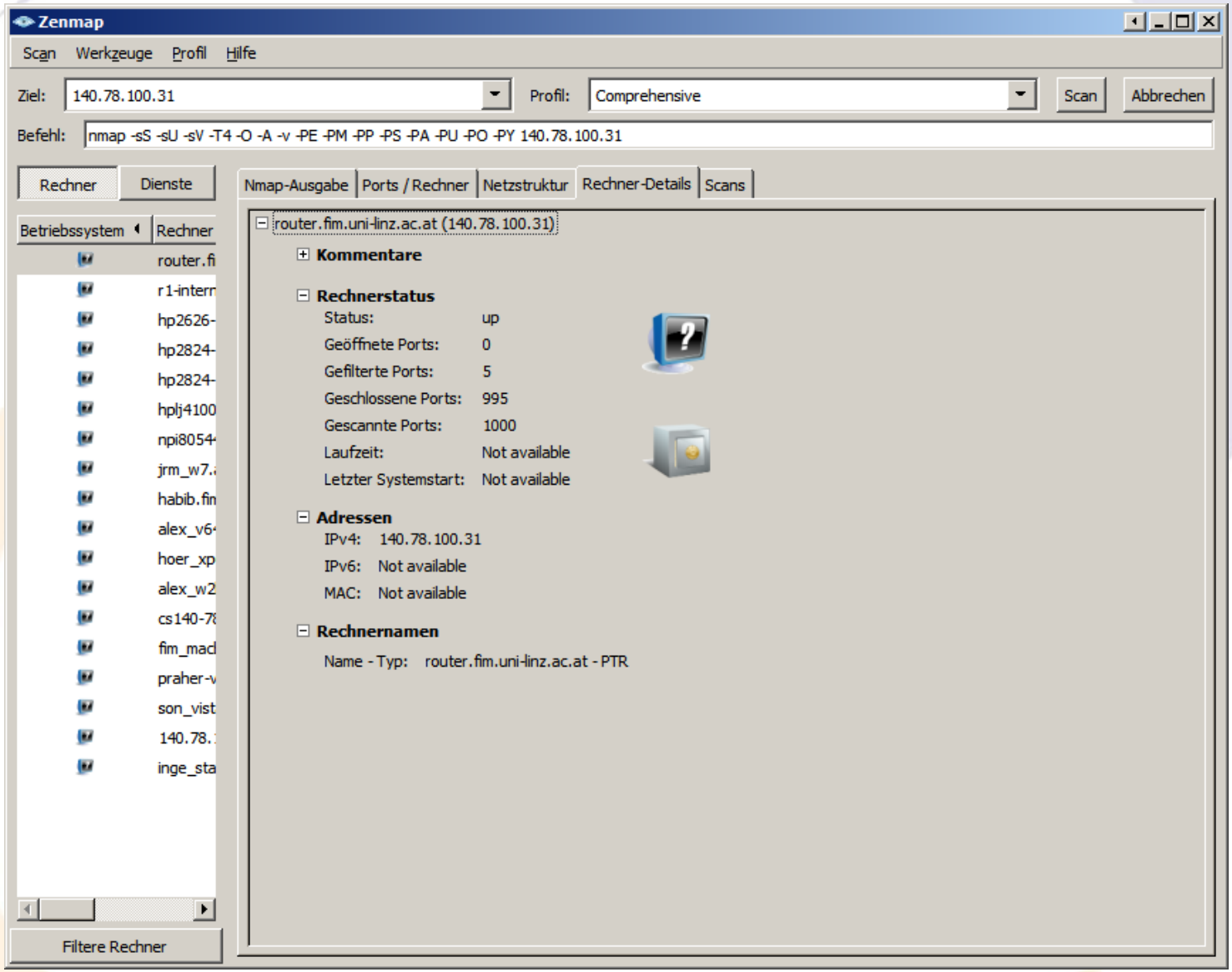
Sample result: NMap local subnet scan



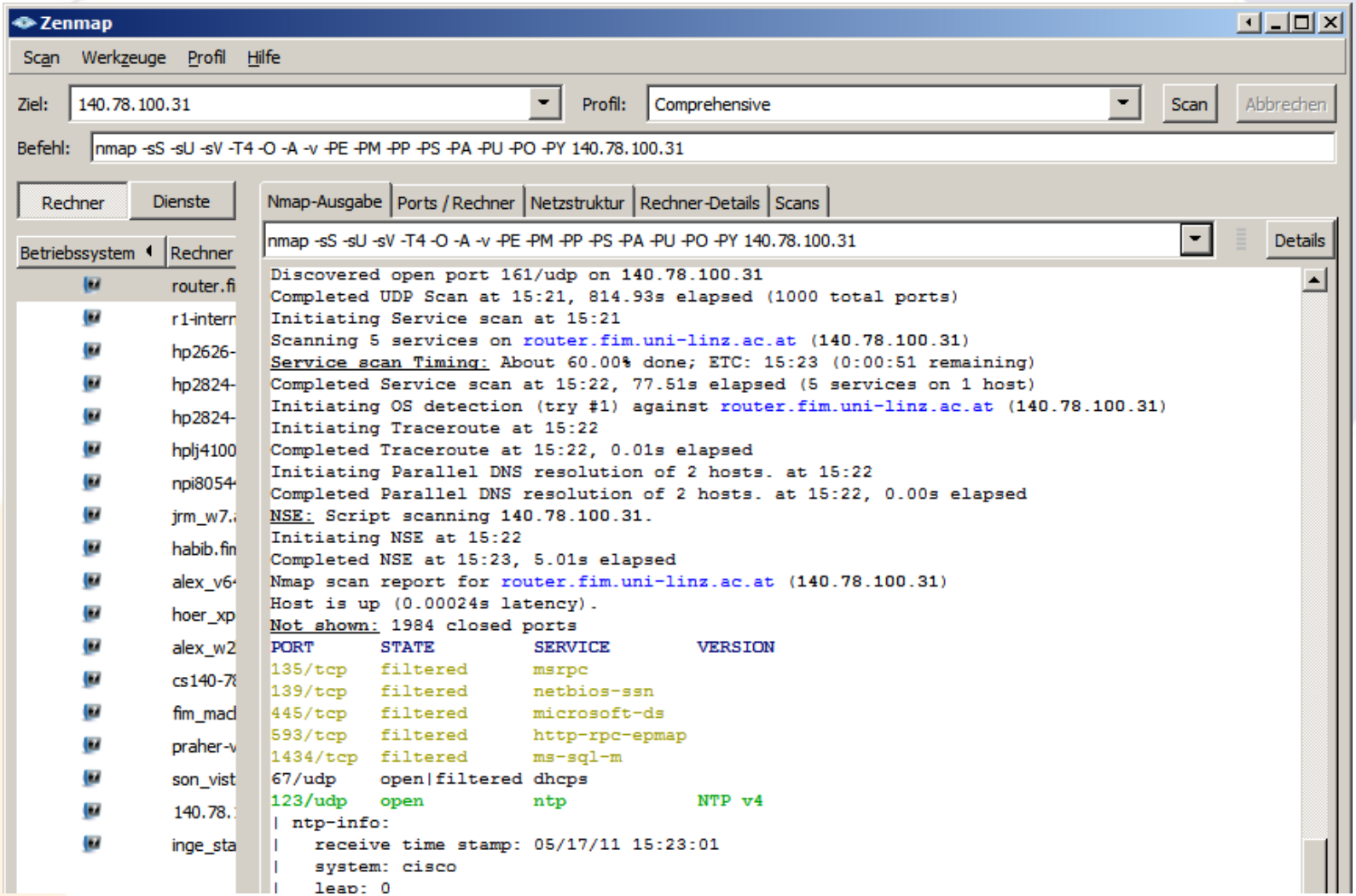
Sample result: NMap info



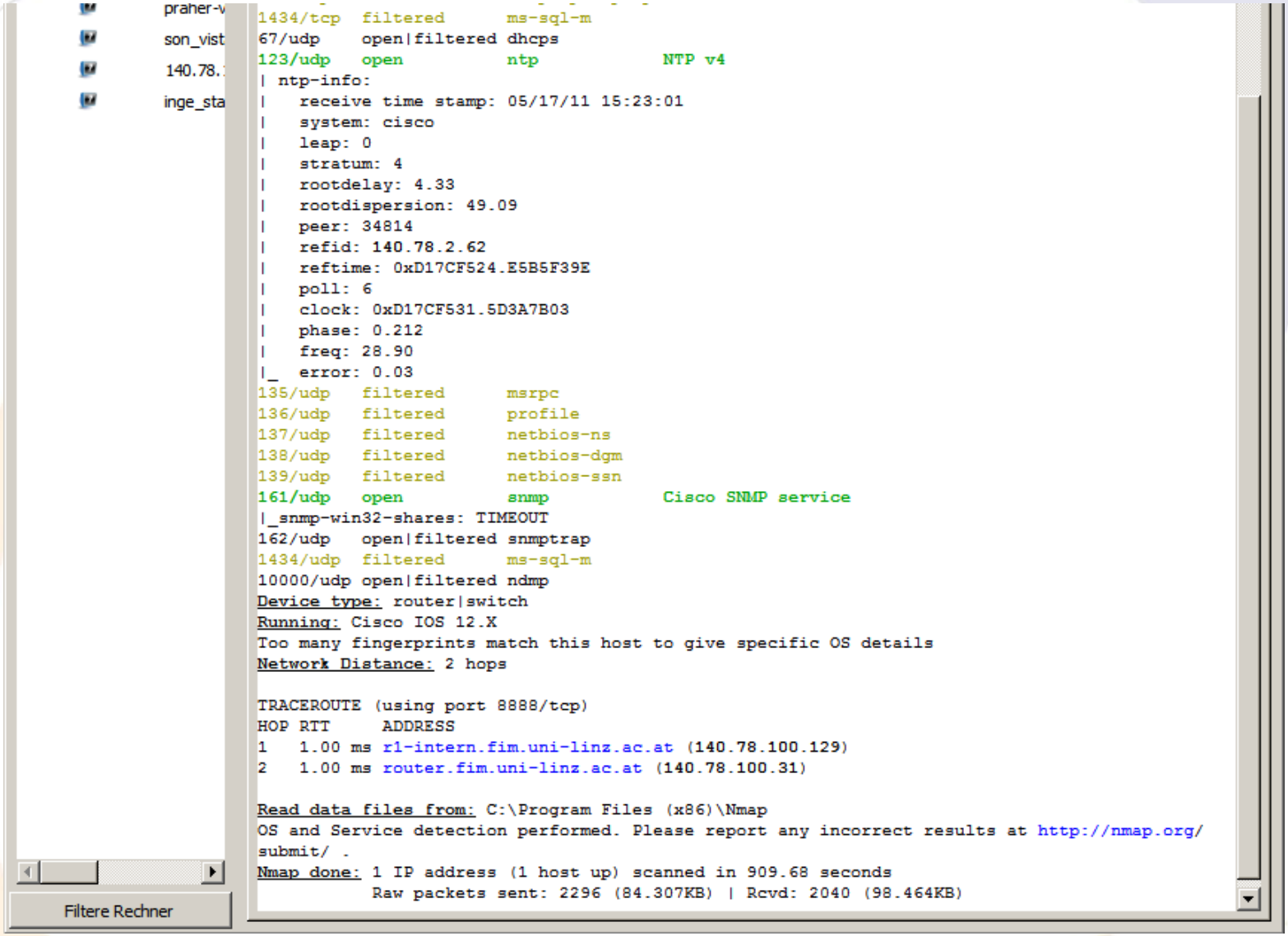
Sample result: NMap info



Sample result: NMap info



Sample result: NMap info



Google Cache

- The cache gives you access to old/removed content
  - → Which might still be applicable!
- Attention: Surfing the cache will still touch the server
  - → E.g. images are loaded from the “source”
- Way around: View the text-only version
  - → Add “&strip=1” to the search URL
- Not necessarily complete: Some elements or pages might not be cached (recently/at all)
  - → Also: Only the last version is available!

Google cache: Tasks

- Visit the Google cache for the FIM course homepage
  - » Hint: Search words “fim linz lva teaching”
  - → Check where the FIM logo comes from and what this would mean regarding traces of your actions
    - » How can you prevent this? Test and document it!
  - → Identify the date of this version
  - → Compare this version with the original one
    - » How would you do this?
    - » Note: We want a real comparison, not “looks the same”!
    - » What problems do occur? How can you reduce them?
- Investigate, whether Bing and Yahoo do have a similar feature; if yes, try it and document the differences!
  - → Both in features and for the specific page above!

Web archive: Tasks

- Web Archive (=Wayback Machine) is a permanent archive of the WWW (not: The Internet!)
  - → Find out which pages are being archived, and how often!
  - → What is archived for a web page? Check the logo!
  - → How reliable is it, i.e. which modifications take place?
- “I don’t want my page in there!”
  - → What can you do?
  - → Is this permanent?
- Try the archive with the following URL: http://www.fim.uni-linz.ac.at/Lva/default.htm
  - → What is the oldest version?
    - » Is this really the oldest one?
  - → Try to get the page without any additions (Wayback-header)!
    - » Hint: Search the FAQ!

Web archive: Solution

- Not everything is archived: Often only the web page (=HTML) alone, but not any images, …
  - → Especially not if from a different domain!
- Exclusion: By robots.txt file
  - → According to posts this is not permanent: “blocked” pages are just not shown, but not deleted!
  - → Later on removed → Content is visible (again)!
  - → Might lead to “new” content being not retrieved/stored
- Pages are rewritten (e.g. links) → This is not a forensic copy!
  - → “Original” version: Append “id_” to date/number
  - → Note: Images are then retrieved from the **current** server!

DNS/WhoIs

- Find a web-based tool for DNS information
  - → Investigate the owner of “www.jku.at”
    - » But think about this question before entering it!
  - → Can you also find the history of this domain?
    - » How would this be possible?
  - → Who owns this domain?
- Get information on the host “www.jku.at”
  - → Both via web tools as well as your own computer!
    - » And repeat this at home from within your private network!

DNS/WhoIs

- http://whois.domaintools.com
- www.jku.at is useless: Only „jku.at“ is in the NIC.at!
  - → Regarding www: Ask the JKU!
- History: Not accessible
  - → Ask the NIC.at (doubtful whether it even exists)
  - → Or use a commercial database (unclear whether included)
  - → You would have to regularly store a copy
- Owner: “Johannes Kepler Universitaet“
- www.jku.at
  - → Might have a different IP from inside the university and outside
  - → Outside: Proxies might be involved (not necessarily visible!)

DNS/WhoIs – MX records

- E-Mail information
  - → Where would E-Mails to “michael.sonntag@jku.at” be sent?
    - » And where so “sonntag@fim.uni-linz.ac.at”?
  - → How would you find this out?
  - → Explain the difference between this and the information about “www.jku.at”!
  - → From where (which IP address) would you expect to receive E-Mails sent from this address?
    - » Is there any possibility to find out?
- MX Lookup from within the institute (see next slide):
  - → Why the difference?
    - » Explain it!
    - » Discuss why this is important for computer forensics!
  - → What does this mean for E-Mail header interpretation?

DNS/WhoIs – MX records

```
C:\Windows\system32\cmd.exe - nslookup
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\michael>nslookup
Default Server:  edc1.ads2-fim.fim.uni-linz.ac.at
Address:  140.78.100.119

> set type=mx
> jku.at
Server:  edc1.ads2-fim.fim.uni-linz.ac.at
Address:  140.78.100.119

Non-authoritative answer:
jku.at  MX preference = 10, mail exchanger = mail2.edvz.uni-linz.ac.at
jku.at  MX preference = 10, mail exchanger = mail1.edvz.uni-linz.ac.at
jku.at  MX preference = 5, mail exchanger = mail3.edvz.uni-linz.ac.at

mail2.edvz.uni-linz.ac.at       internet address = 140.78.3.69
mail1.edvz.uni-linz.ac.at       internet address = 140.78.3.68
> fim.uni-linz.ac.at
Server:  edc1.ads2-fim.fim.uni-linz.ac.at
Address:  140.78.100.119

fim.uni-linz.ac.at      MX preference = 20, mail exchanger = mail2.edvz.uni-linz
.ac.at
fim.uni-linz.ac.at      MX preference = 5, mail exchanger = smtp.fim.uni-linz.ac
.at
fim.uni-linz.ac.at      MX preference = 10, mail exchanger = mail1.edvz.uni-linz
.ac.at
mail2.edvz.uni-linz.ac.at       internet address = 140.78.3.69
smtp.fim.uni-linz.ac.at internet address = 140.78.100.121
mail1.edvz.uni-linz.ac.at       internet address = 140.78.3.68
>
```

DNS/WhoIs – MX records

root@mail:~

```
[root@mail ~]# dig -t MX fim.uni-linz.ac.at

; <<>> DiG 9.7.4-RedHat-9.7.4-1.el5 <<>> -t MX fim.uni-linz.ac.at
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9067
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 8

;; QUESTION SECTION:
;fim.uni-linz.ac.at.            IN      MX

;; ANSWER SECTION:
fim.uni-linz.ac.at.     5532    IN      MX      20 mail2.edvz.uni-linz.ac.at.
fim.uni-linz.ac.at.     5532    IN      MX      10 mail1.edvz.uni-linz.ac.at.

;; AUTHORITY SECTION:
fim.uni-linz.ac.at.     5532    IN      NS      alijku01.edvz.uni-linz.ac.at.
fim.uni-linz.ac.at.     5532    IN      NS      ns1.fim.uni-linz.ac.at.
fim.uni-linz.ac.at.     5532    IN      NS      ns2.jku.at.
fim.uni-linz.ac.at.     5532    IN      NS      ns2.fim.uni-linz.ac.at.

;; ADDITIONAL SECTION:
mail1.edvz.uni-linz.ac.at. 1946 IN      A       140.78.3.68
mail1.edvz.uni-linz.ac.at. 1946 IN      AAAA    2001:628:2010:2::68
mail2.edvz.uni-linz.ac.at. 1932 IN      A       140.78.3.69
mail2.edvz.uni-linz.ac.at. 1932 IN      AAAA    2001:628:2010:2::69
ns1.fim.uni-linz.ac.at. 7177    IN      A       140.78.100.48
ns2.fim.uni-linz.ac.at. 7177    IN      A       140.78.100.49
ns2.jku.at.             46599   IN      A       140.78.3.62
alijku01.edvz.uni-linz.ac.at. 1932 IN   A       140.78.2.62

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Oct 10 11:19:11 2011
;; MSG SIZE  rcvd: 318
```

DNS/WhoIs – MX records

- MX for “jku.at”: mail{1,2,3}.edvz.uni-linz.ac.at
  - → Primarily mail1 and equally to mail2 and mail3
- MX for “fim.uni-linz.ac.at”: smtp.fim.uni-linz.ac.at or mail1/mail2.edvz.uni-linz.ac.at
  - → Primarily to FIM, then mail1, then mail2
  - → Different view from the outside: Everything must go through the university mail server and is then sent on!
- Outgoing: Sent from the FIM mailserver to destination directly, i.e. NOT using the JKU mailserver!
- Different views are possible and do exist

DNS/WhoIs – MX records

- Why? JKU can delegate subdomains itself. This happened to fim.uni-linz.ac.at
  - → Note: Different domain, but principles for “jku.at” apply to “uni-linz.ac.at” as well!
- Received E-Mails: Same address
  - → Especially: FIM (“smtp”!)
  - → But: Not necessarily! Outbound mails might not be scanned and just be sent from any internal address (JKU has public IPs; else: NAT!)
    - » JKU is large: Might have a separate server for sending

Wireshark

- If you want to see the real traffic from/to a computer, you need to listen in on the wire!
  - → Listening on the computer itself is not a good idea
    - » Requires time → Modification of behaviour
    - » Binaries (or even the network driver) might be modified
  - → Listening on the default gateway/router
    - » Will only show traffic going there/outside
    - » Internal traffic will mostly go directly (no bus topology + switch)
  - → What can you do?
    - » Special wiretap devices (=copy traffic to a second port)
    - » Network monitoring port on switches (=copy traffic on spec. port)
    - » Listen on the system itself or on the router ☺
- Software for this:
  - → Wireshark: UI + interpretation of protocols + …
  - → tcpdump: Unix commandline tool with little additional functions

Wireshark

- Wireshark is a network sniffer
  - → Available for Windows and Linux
- It will make a “copy” of every incoming and outgoing packet and present it to you
  - → This would not be that useful…
- It also parses a lot of protocols
  - → So no binary display (also available!), but
  - → layer 3 display (IP addresses, port numbers, …),
  - → up to layer 5 (actual http content as text/binary file)
- Practical problem: Network traffic is very large & frequent
  - → Filtering is an absolute necessity or anything useful will get lost in a torrent of uninteresting traffic!

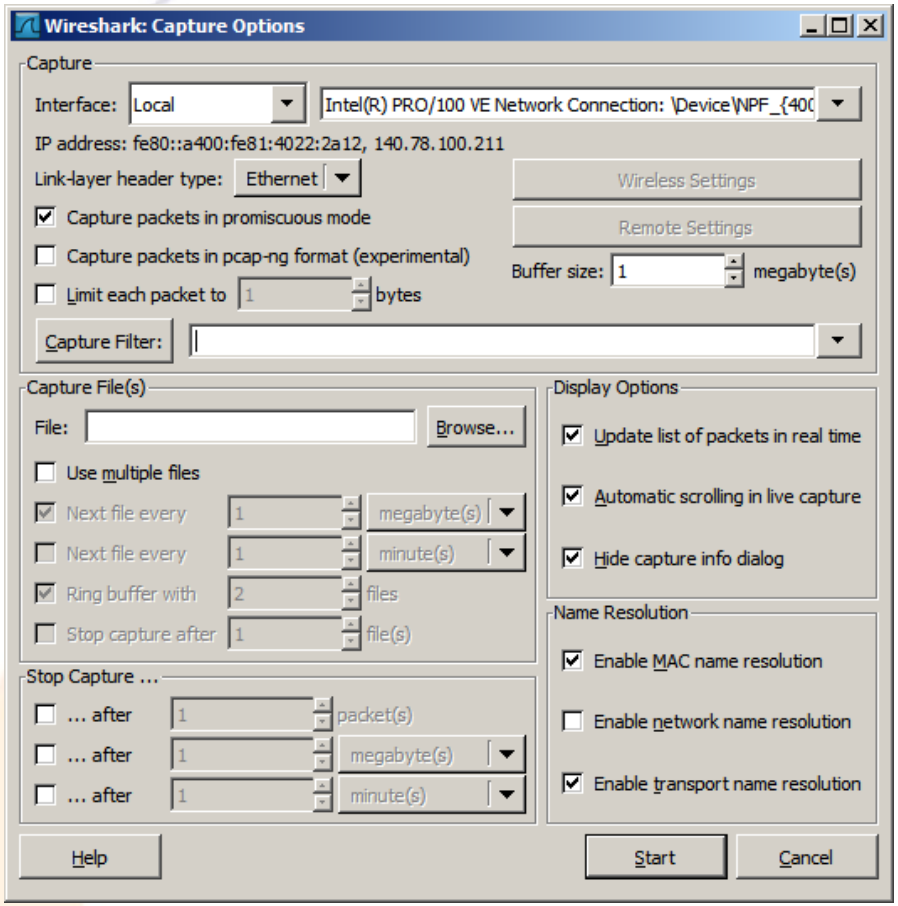
Wireshark
Common display filtering expressions (1)

- Operators: == != < > <= >= && || ^^ !
  - → […] or […:…] or […-…]: Offset / Offset:Length / Offset-End
    - » Only possible as comparison, e.g. eth.src[0:3]==08:15:47!
- Layer 1/2: frame.??? / eth.???, arp.???, ppp.???
  - → Usually not very interesting
- Layer 3: ip.???, ipv6.???, icmp.???, icmpv6.???
  - → Examples ip.???: .src, .dst, .addr, .src_host, .dst_host, .host, .flags, .fragment, .len, .proto, .ttl
    - » ip.tos, ip.tos.cost, ip.tos.delay, ip.tos.precedence, ip.tos.reliability, ip.tos.throughput
  - → Examples icmp.???: .code, .type, .mtu
- Layer 4: tcp.???, udp.???
  - → Examples tcp.???: .syn, .ack, .fin, .checksum, .flags, .len, .srcport, .dstport, .port, .time_delta, .window_size
  - → Examples udp.???: .srcport, .dstport, .port, .length

Common display filtering expressions (2)

- Layer 5: http, ospf, rip, …
  - → Examples http.???
    - » .accept, .accept_encoding, .accept_language, .cookie, .date, .host, .last_modified, .location, .referer, .request, .request.method, .request.uri, .response, .response.code, .server, .set_cookie, .user_agent, .transfer_encoding
- Attention: This means that packets have been received and are stored, but will not be shown in the graphical UI!
  - → There is also the possibility of filtering-before-storing
  - → These are “capture filters”, which use the syntax on libpcap (or tcpdump, which is the same)
    - » Examples: ether host 08:15:47:11:CA:FE
      - – Display filter for the same: eth.addr=08.15.47.11.CA.FE
    - » Note: Too many packets to store → Some might be lost
    - » But: Capture filter dropped it → Gone forever

Wireshark

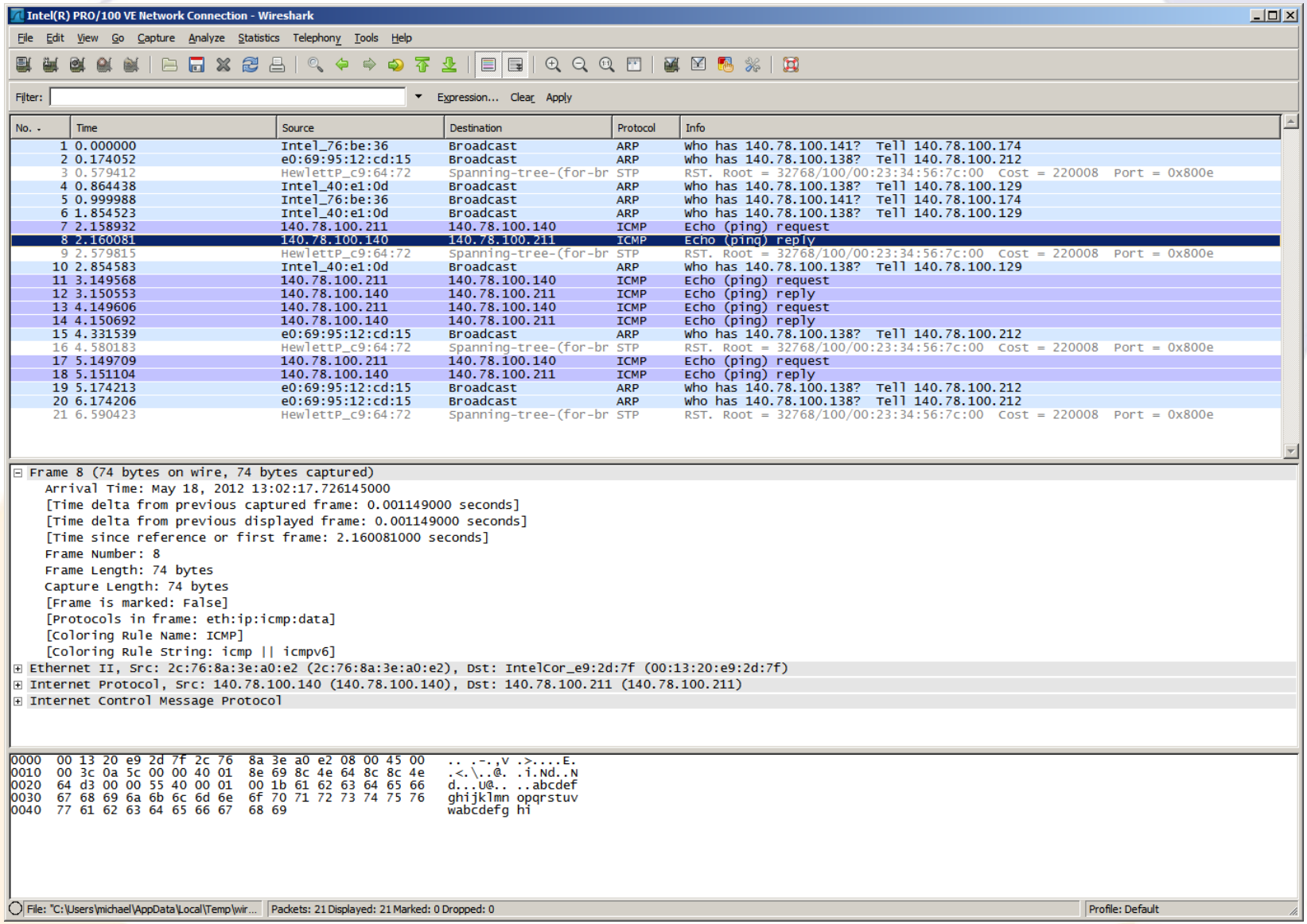


- Interface: Select where to listen
- Capture filter: Throw away packets before handling/storing them
- Capture file: How/where to store data; especially useful for keeping a history (e.g. last 60 minutes), timing, ..
- Buffer size: 1 MB can be too small for fast interface, much traffic and large packets!
- Display options: Personal prefer.
- Name resolution: Be careful!
  - → This might cause additional traffic!

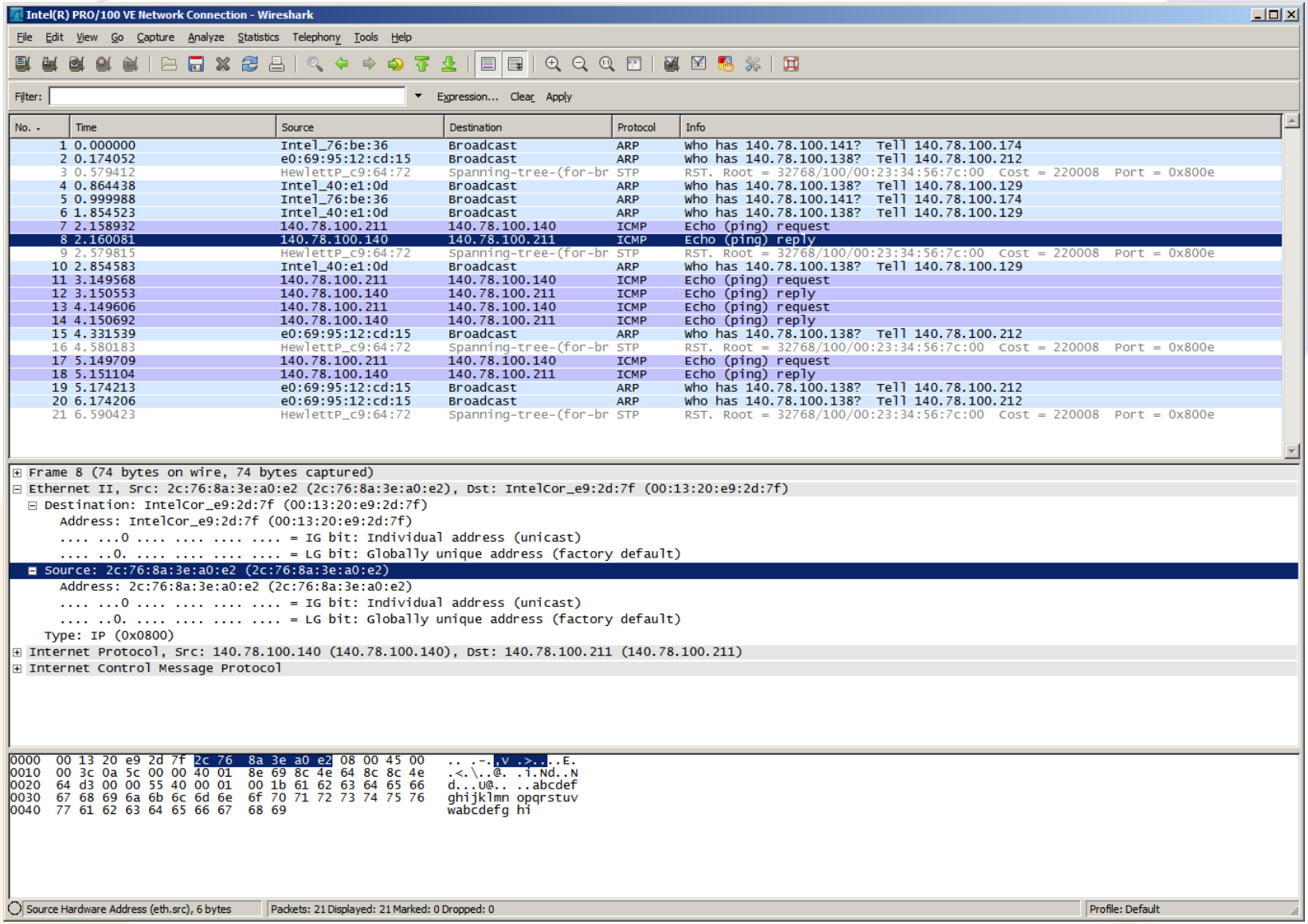
Wireshark

- Usage:
  - → Start program and select interface to monitor
  - → Investigate content while running (difficult) or stop the scan and the start evaluation (store to disk, …)
- Your tasks:
  - → Install Wireshark
    - » Might require reboot for the packet capturing library!
  - → Start a scan of your local interface
    - » Note: Wireless can be difficult/require additional libraries!
  - → Ping your neighbour & analyze the traffic
  - → Navigate to a website & analyze the traffic
  - → Log in to this website through a form (unencrypted)
    - » Analyze the traffic
  - → Do the same as before, but now using a TLS connection!

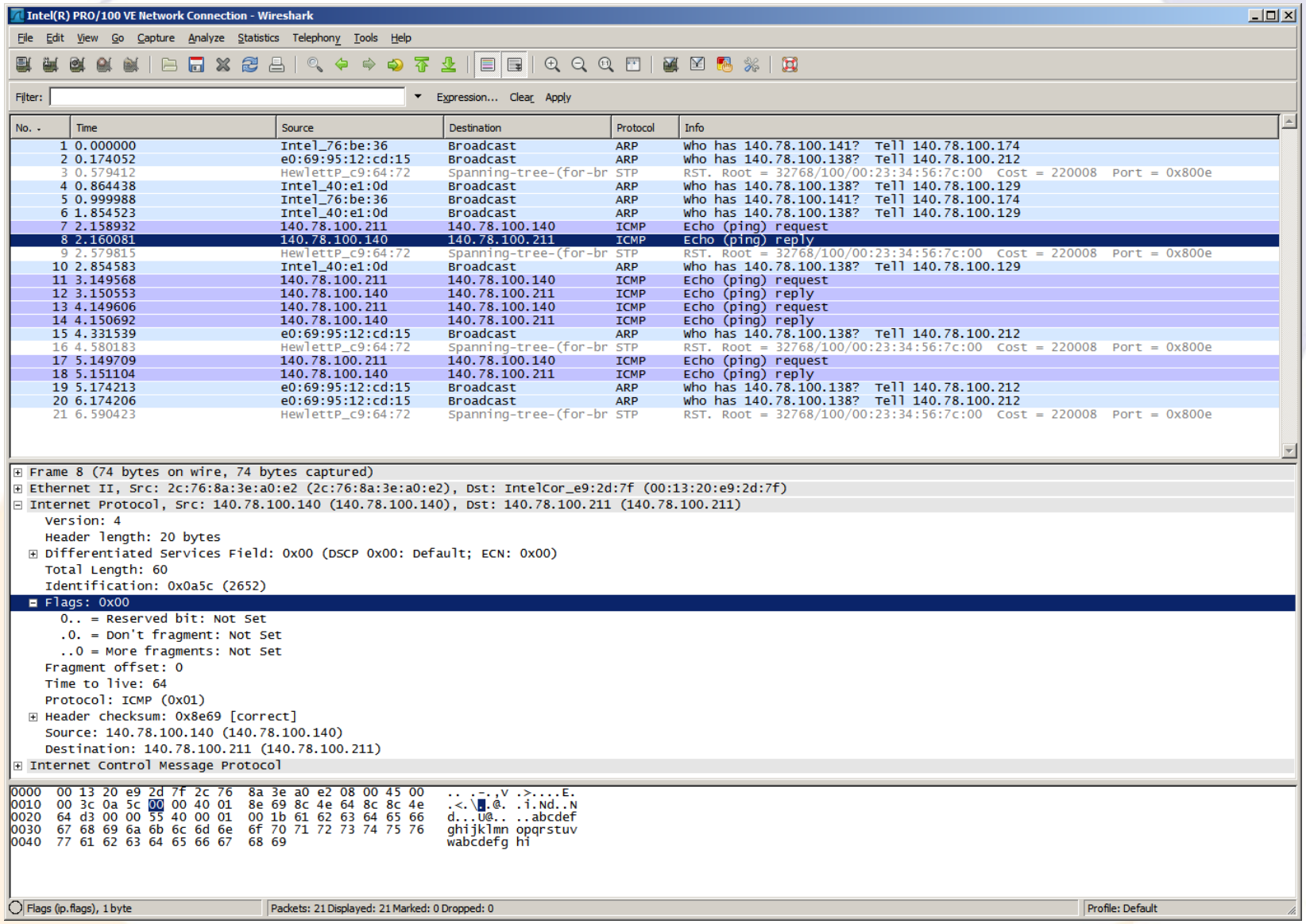
Wireshark Ping



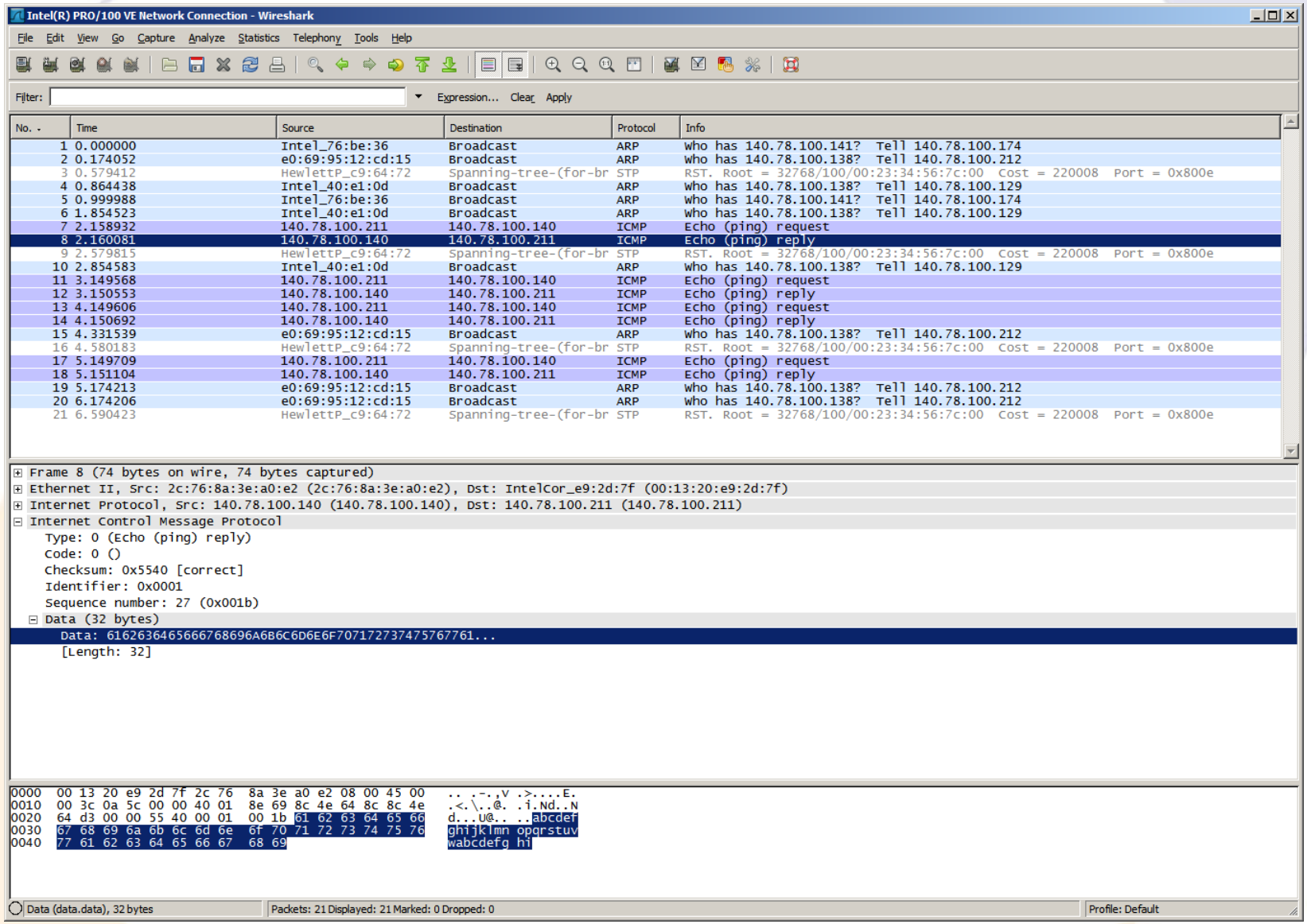
Wireshark Ping



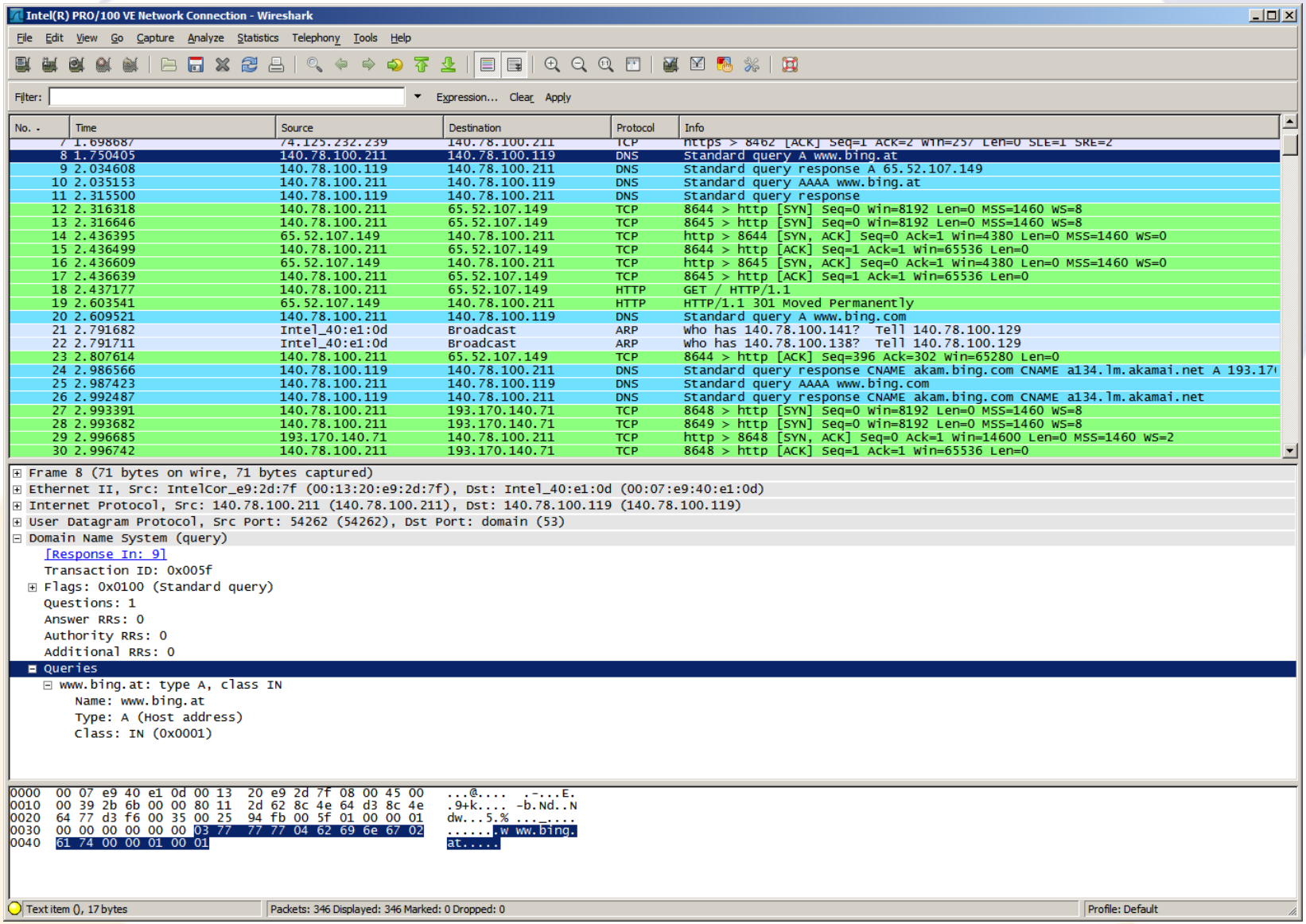
Wireshark Ping



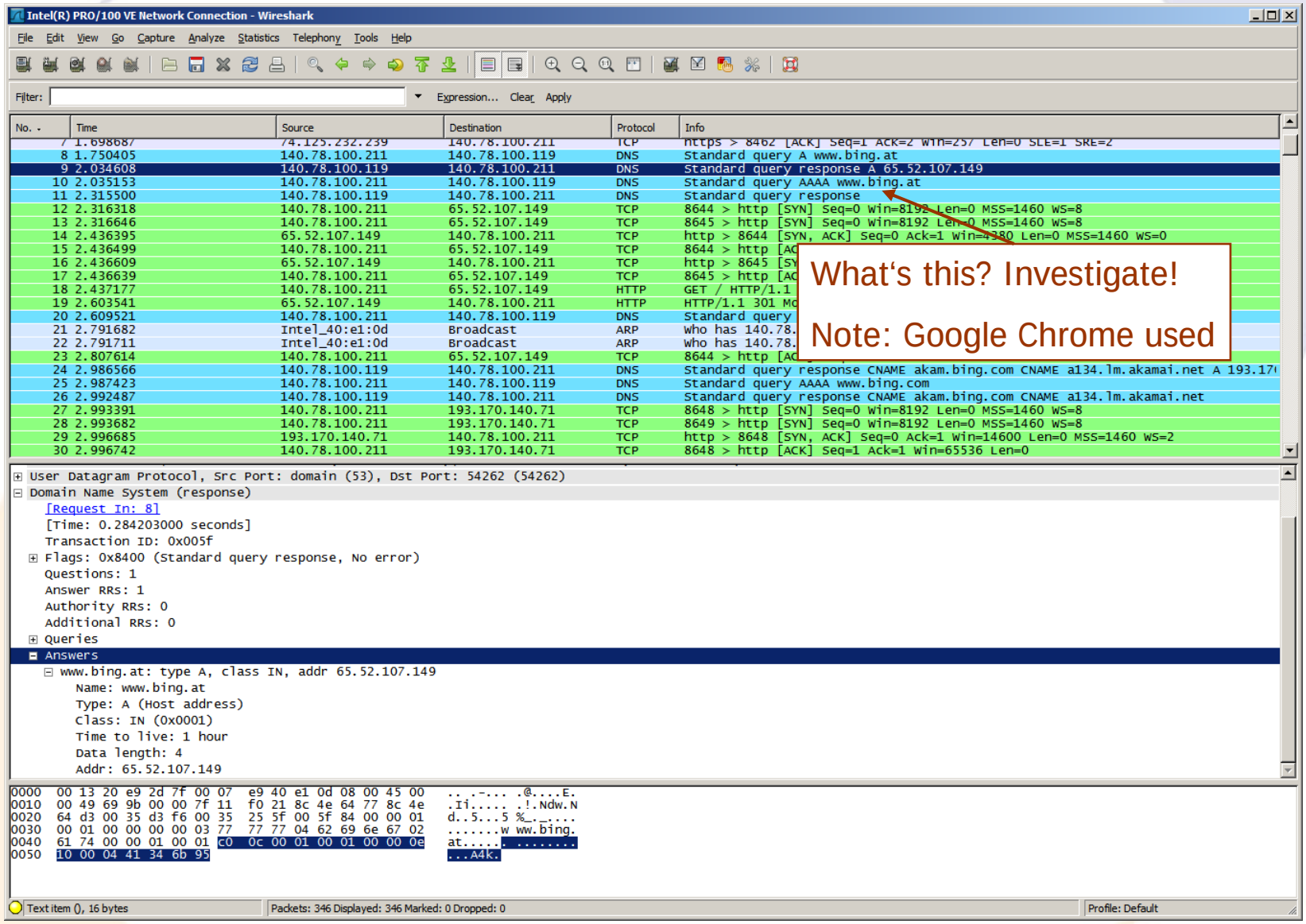
Wireshark Ping



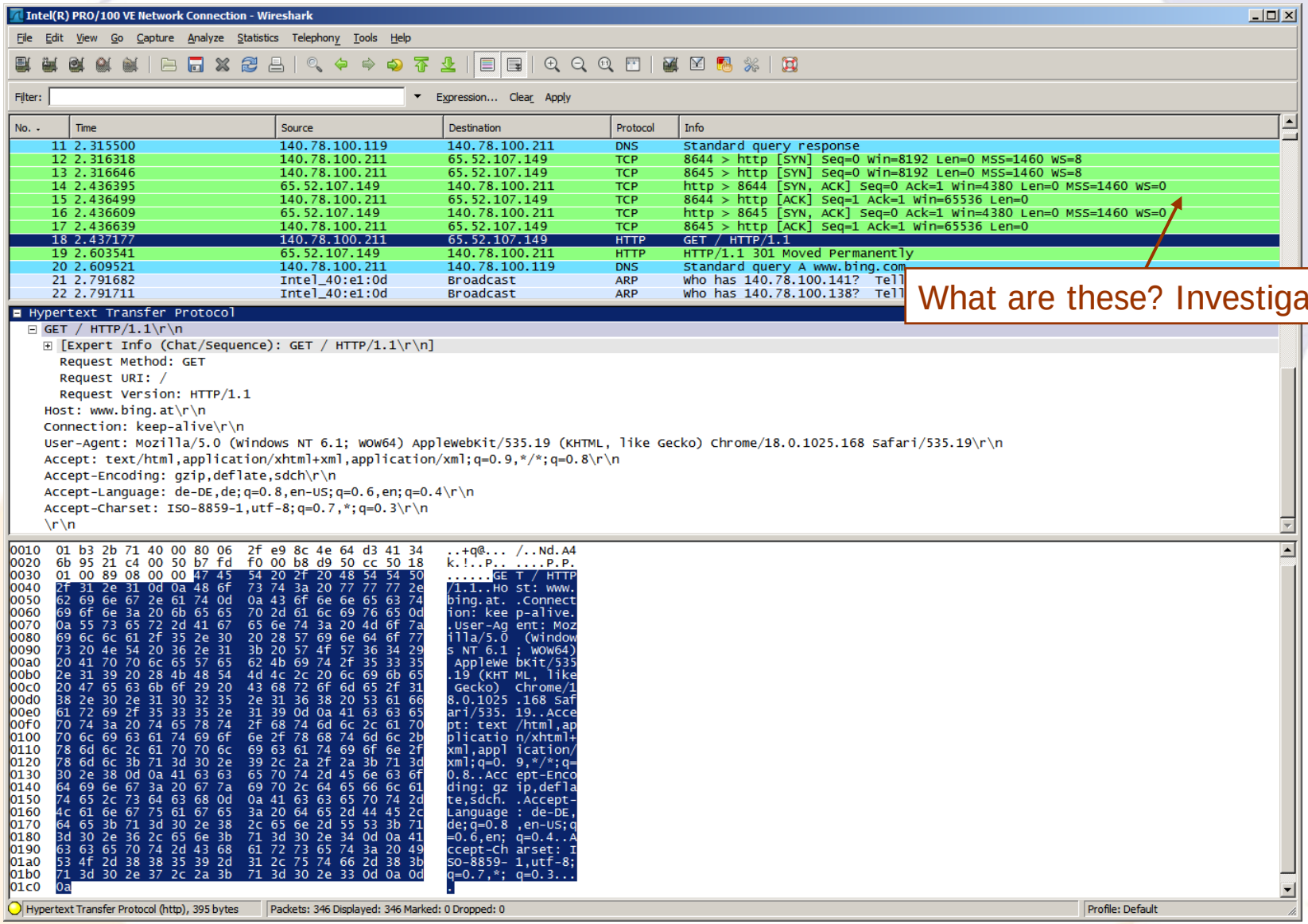
Wireshark
HTTP - DNS



Wireshark
HTTP - DNS

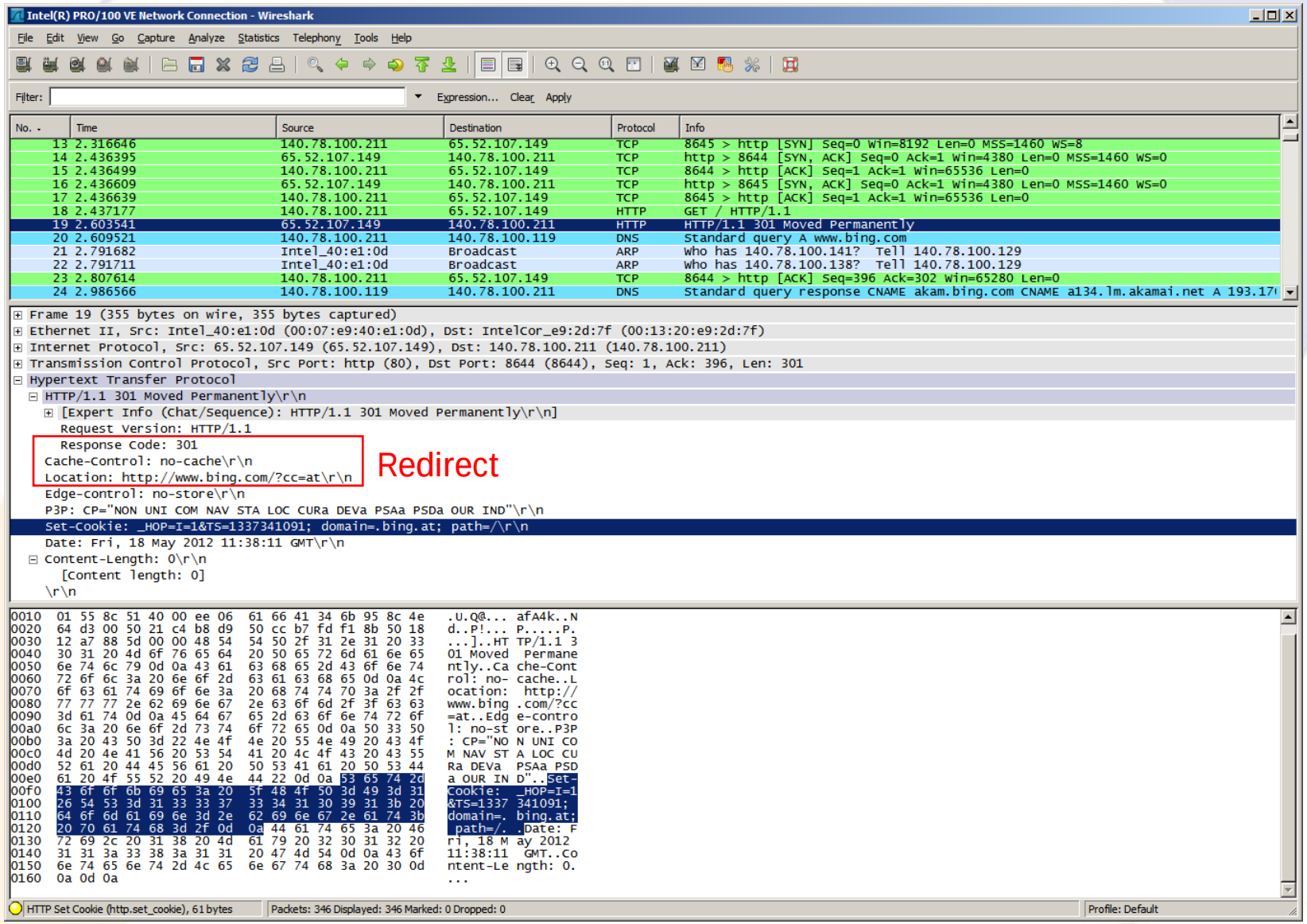


Wireshark
HTTP - Request

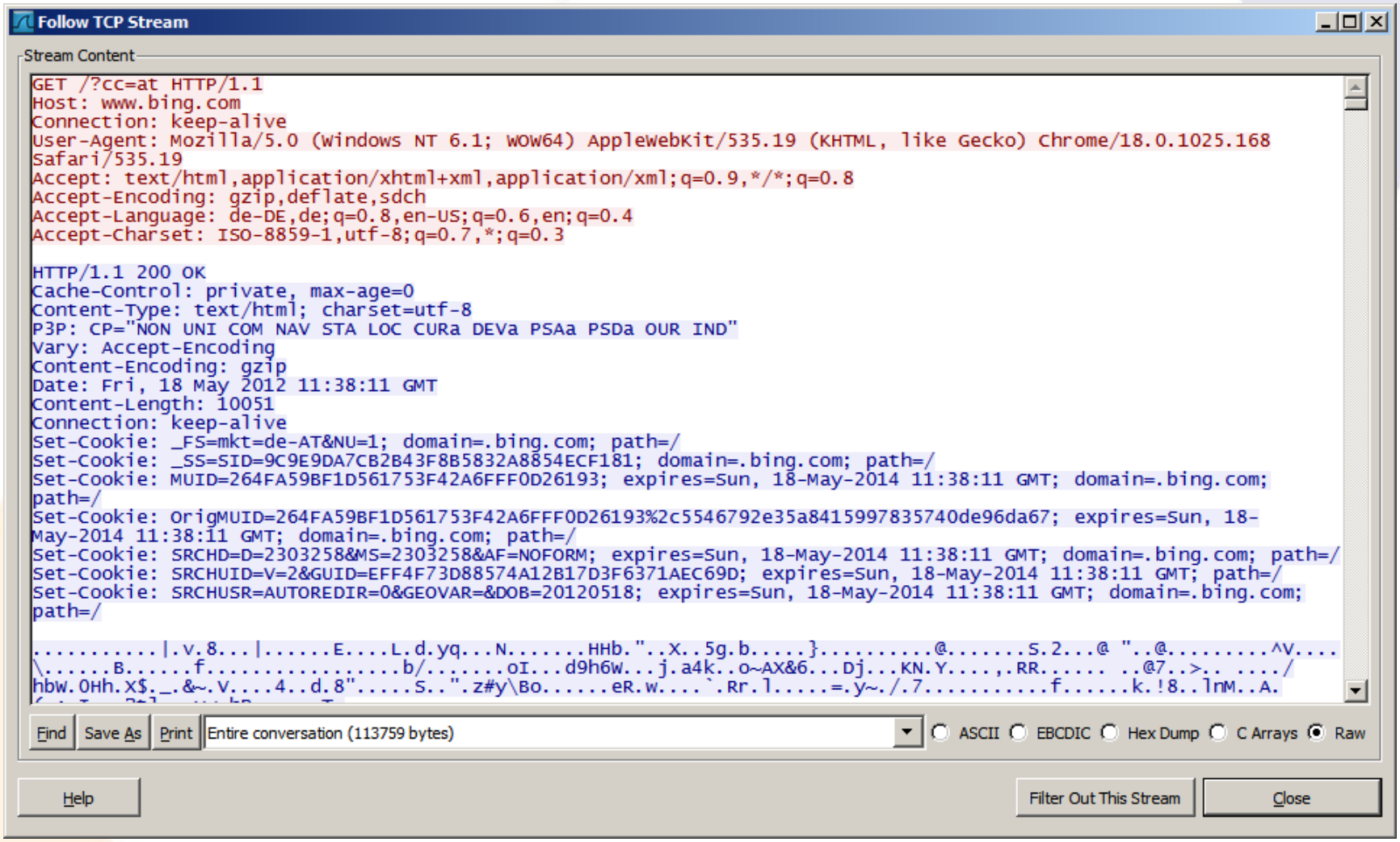


What are these? Investigate!

Wireshark
HTTP - Response



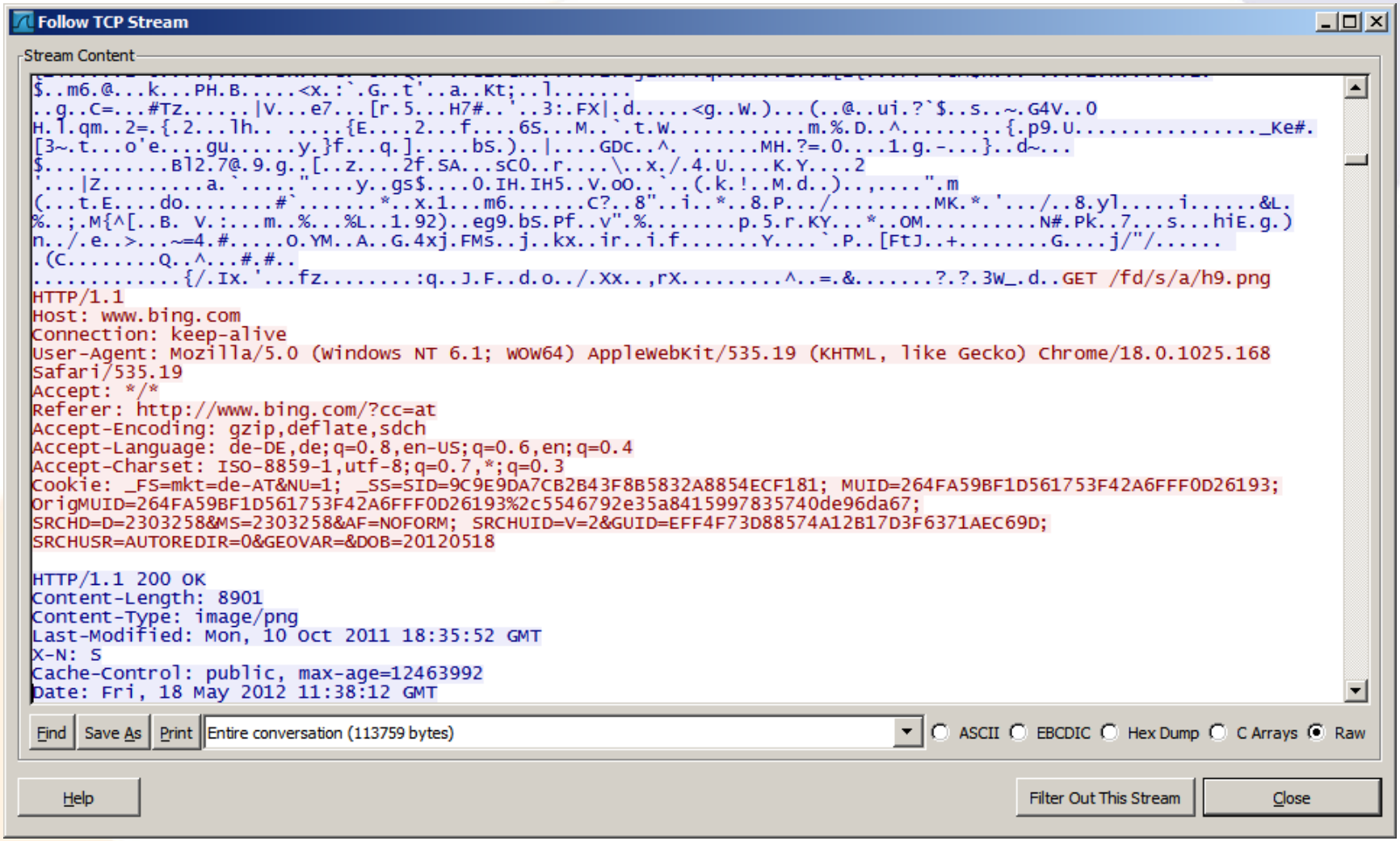
Wireshark
HTTP - Stream



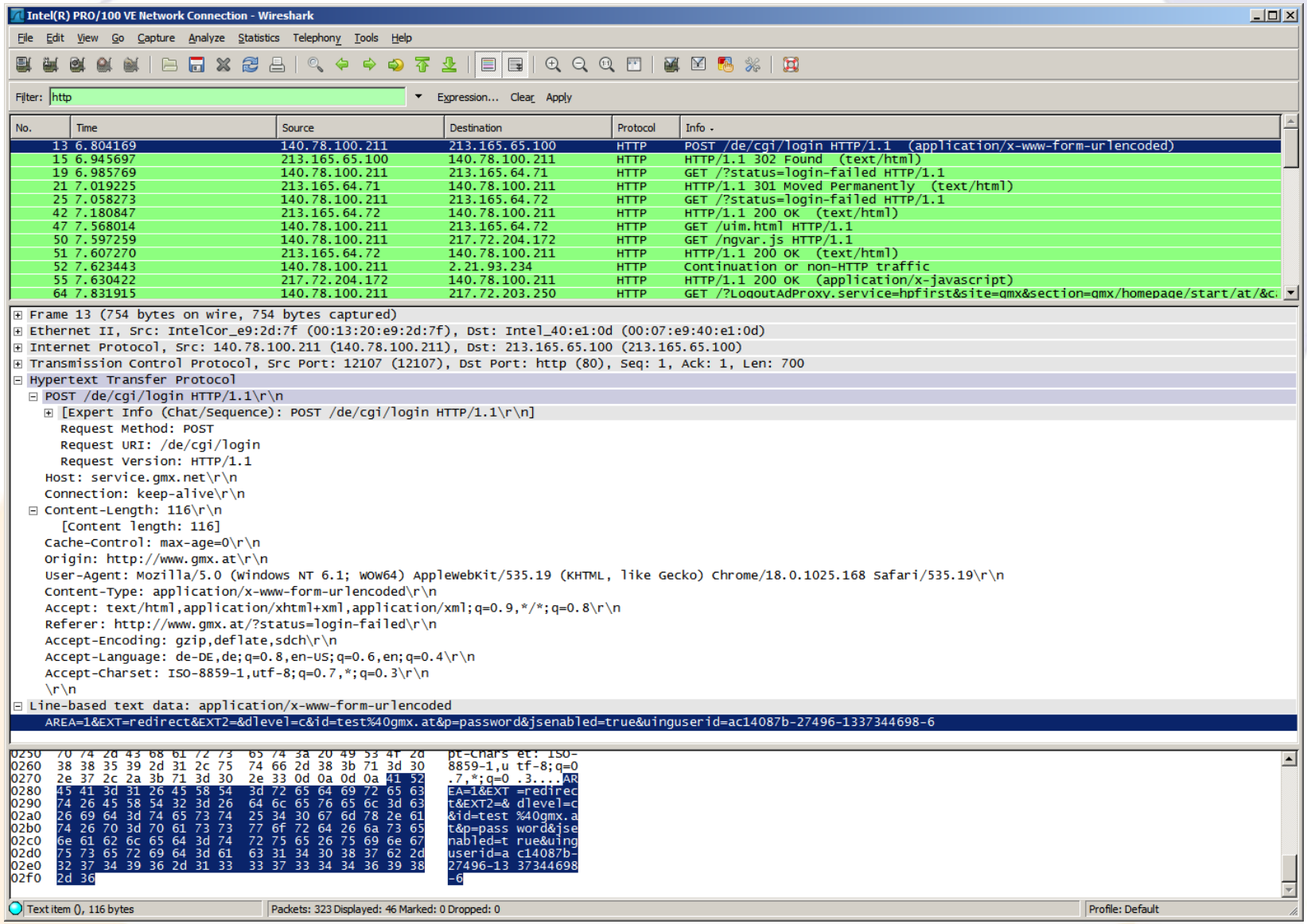
Wireshark
HTTP - Stream

- Keep-alive: Requested by browser and accepted by sender
  - → Result: After the end of the first response, there follows immedaitely the next request and response
- Content-Encoding: gzip
  - → The content would have to be saved as a binary file and then unzipped to access it (selecting & copying won‘t work!)
- Response: Normal response headers, P3P information and lots of cookies!
  - → 7 cookies, but note: we didn’t send even a single one!
    - » Would have been in the request header
  - → Careful: Second request in this stream already knows the headers and does send them with the request!

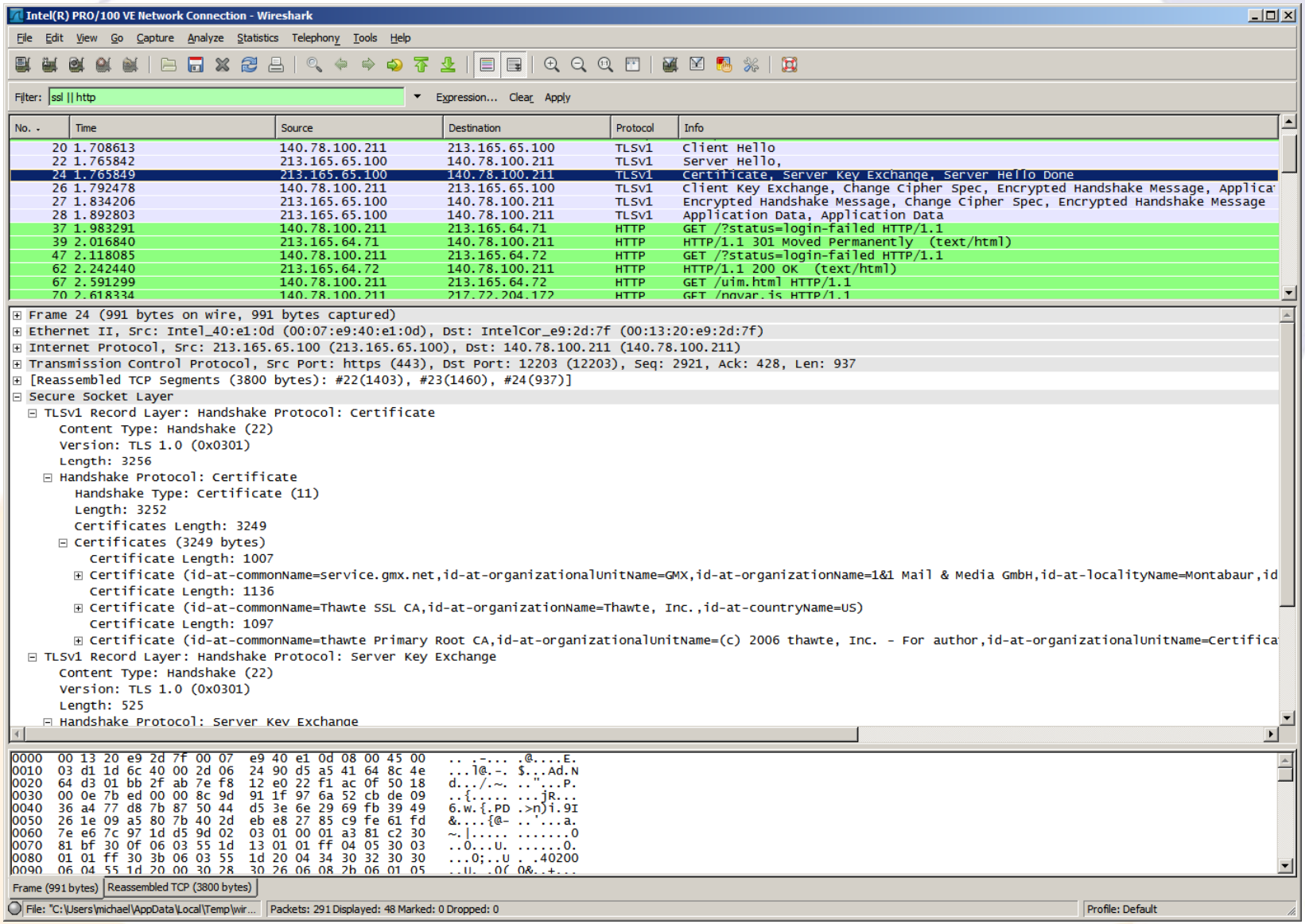
Wireshark
HTTP - Stream



Wireshark
HTTP authentication



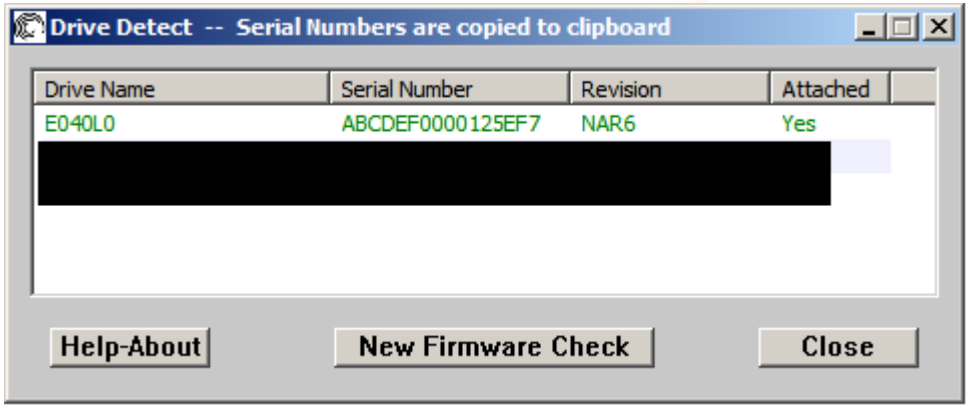
Wireshark
HTTP authentication + TLS



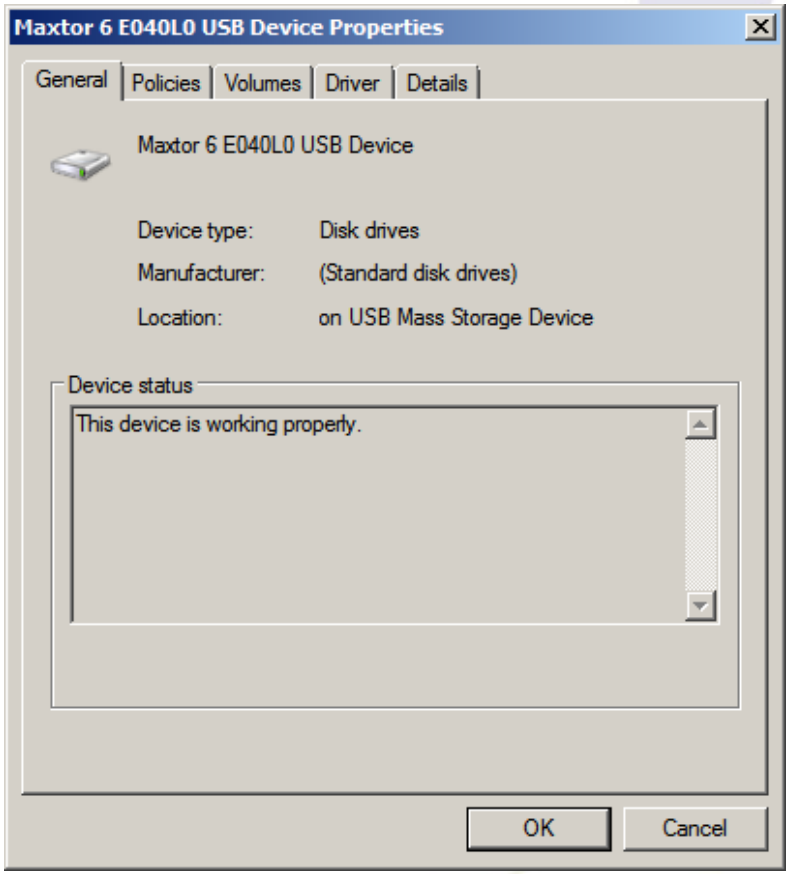
Serial number: Photograph

- Code: NAR61HA0
- 6E040L0711214
- E1245D7N

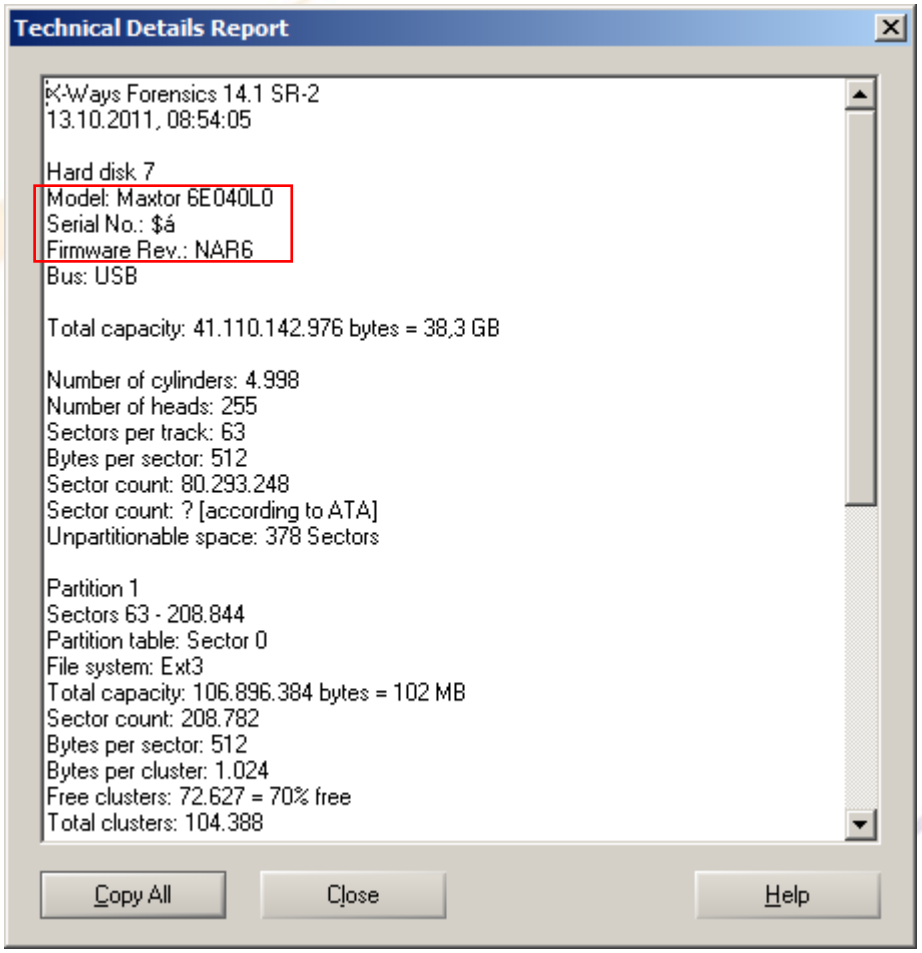
Serial number: According to tools



http://support.seagate.com/firmware/drive_config.html



Serial number: X-Ways Forensic



Serial number: Web information

Seagate
We turn on ideas

Serial Number Locator

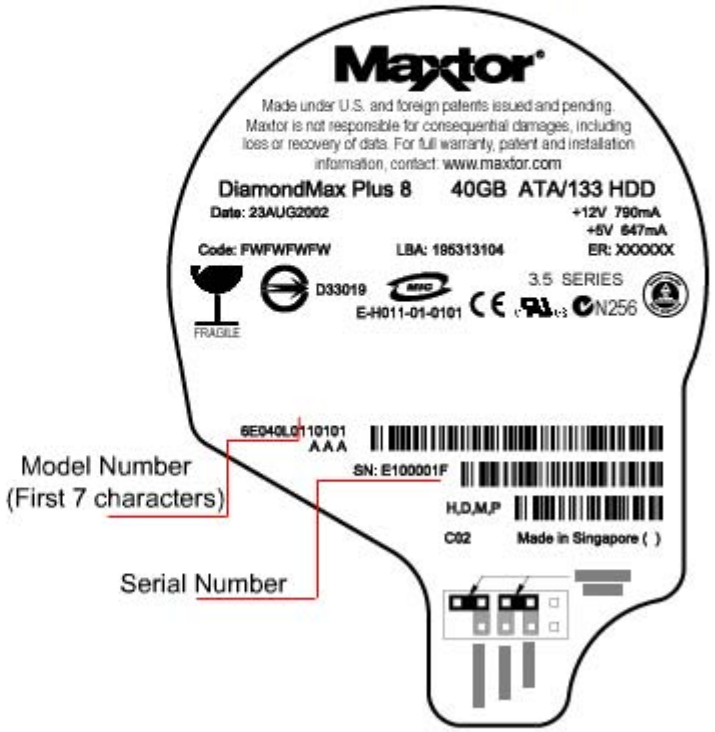
This label type can be found on the following Maxtor drive model:

Diamondmax Plus 8

SeaTools for Windows is a comprehensive, easy-to-use diagnostic tool that helps you quickly determine the condition of the disc drive in your external hard drive, desktop or notebook computer. It includes several tests that will examine the physical media on your Seagate or Maxtor disc drive and any other non-Seagate disc drive. SeaTools for Windows tests USB, 1394, ATA (PATA/IDE), SATA and SCSI drives. It installs onto your system. SeaTools for Windows is completely data safe.

Download SeaTools

Maxtor DiamondMax Plus 8

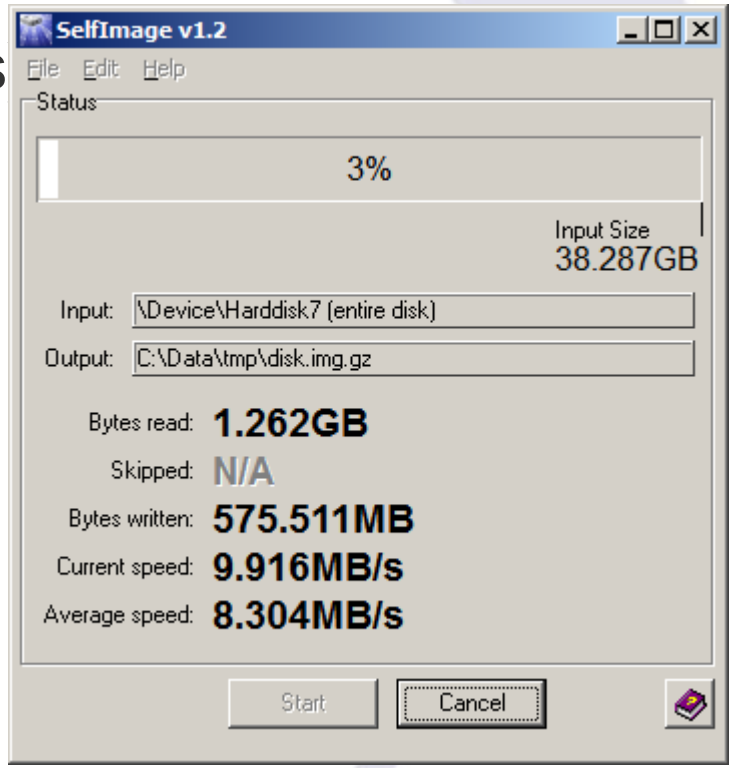


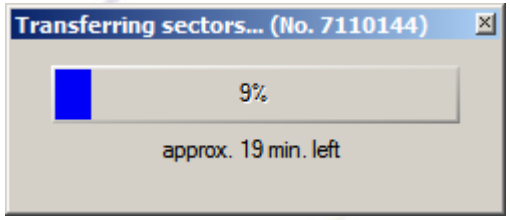
Main Menu Print

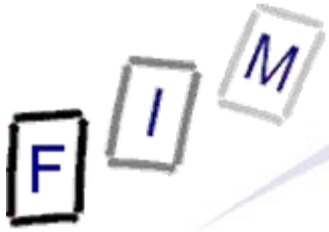
http://support.seagate.com/kbimg/flash/serial_number_locator/SerialNumberLocator.html

Disk image

- Variant A: SelfImage (or other tools
  - → Useful tool, no forensic support
  - → Problem: Finding the correct disk
  - → No timing/estimate
  - → Ca. 500 MB/min
- Variant B: dcfldd
  - → Problem: “Permission denied” on Windows 7
- Variant C: X-Ways Forensic
  - → Only complete drives or logical drives (=has a drive letter); no partitions
  - → Full version needed (or only 200 kB!)
  - → Must be run as Administrator
  - → Ca. 850 MB/min







Questions?

Thank you for your attention!

Literature/Links

- NMap
  http://nmap.org/
- Wayback Machine
  http://www.archive.org/web/web.php
- DomainTools WhoIs
  http://whois.domaintools.com
- MX Toolbox
  http://www.mxtoolbox.com/
- Wireshark
  http://www.wireshark.org/