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

Zenmap

Scan Werkzeuge Profil Hilfe

Ziel: 140.78.100.128/25 Profil: Ping scan Scan Abbrechen

Befehl: nmap -sn 140.78.100.128/25

Rechner Dienste

| Betriebssystem | Rechner |
|---|---|
| | r1-intern.fim.un |
| | hp2824-1a.fim.u |
| | npic3f08e.fim.u |
| | hpljm602.fim.un |
| | praher-vista32. |
| | inge_xp.ads2-fi |
| | 140.78.100.168 |
| | sabine-win7.ads |
| | 140.78.100.206 |
| | 140.78.100.208 |
| | michael_w7.ads |
| | jrm_win7.ads2- |
| | 140.78.100.250 |
| | 140.78.100.251 |

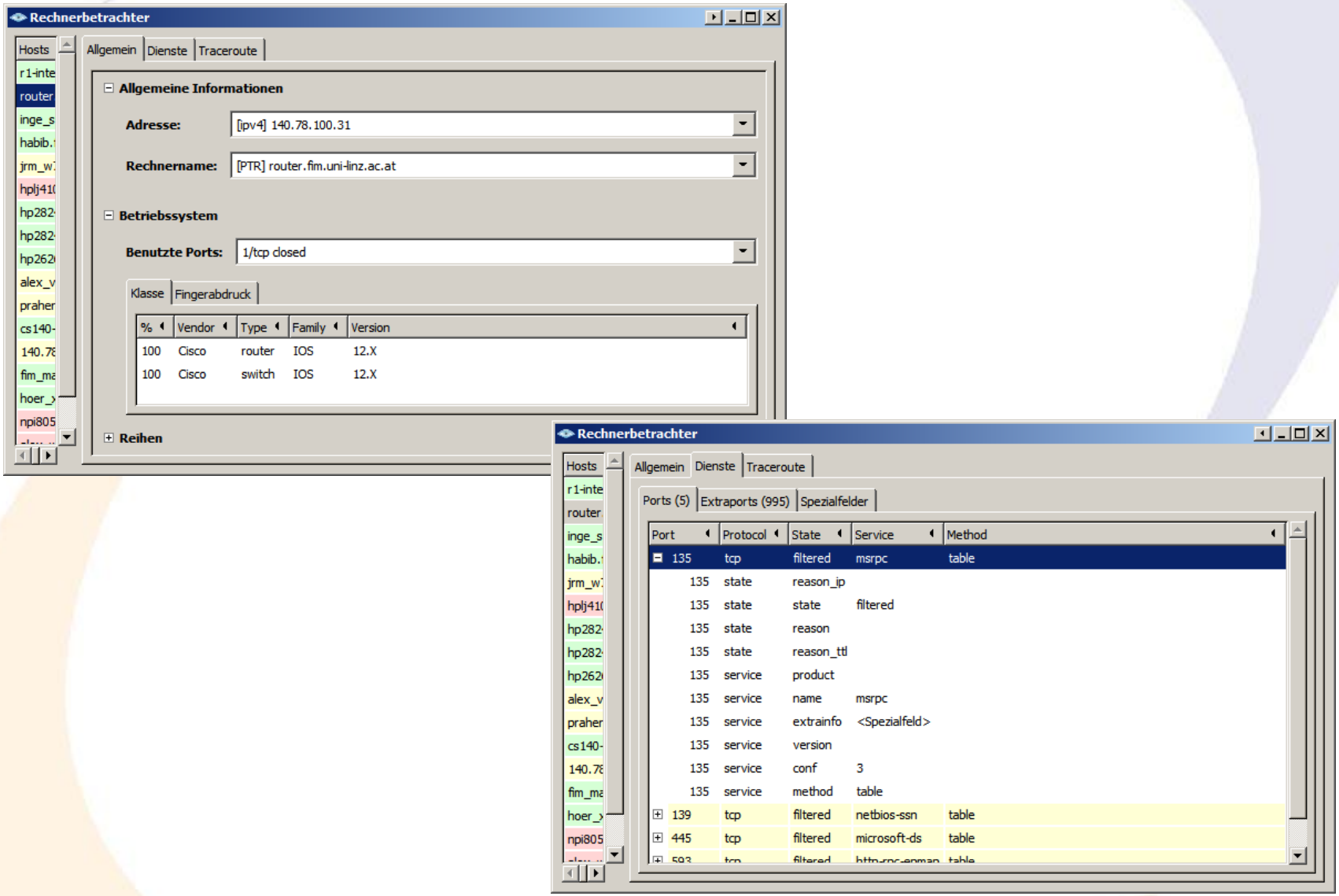
Filtere Rechner

Nmap-Ausgabe | Ports / Rechner | Netzstruktur | Rechner-Details | Scans

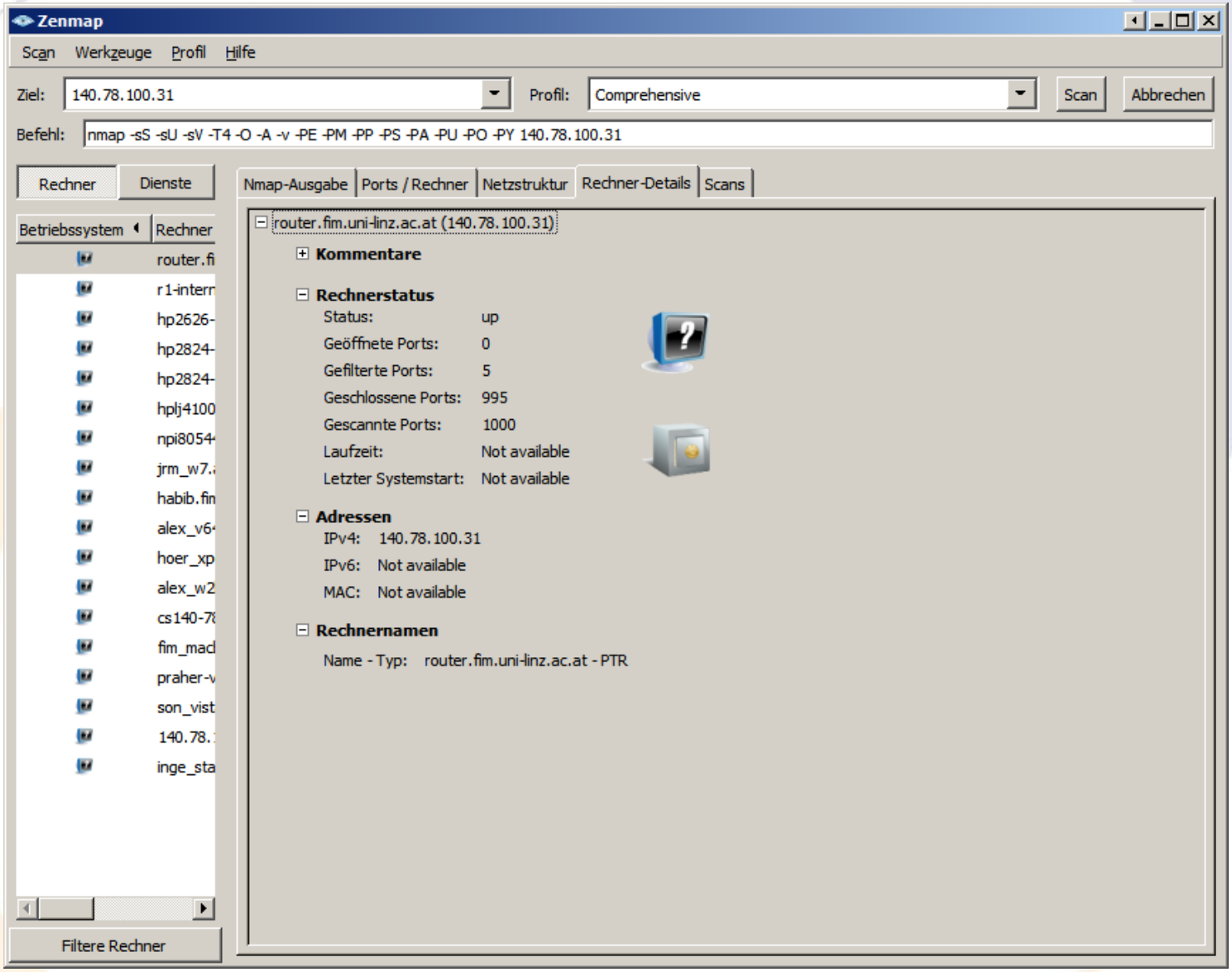
nmap -sn 140.78.100.128/25 Details

```
MAC Address: 00:11:85:C9:62:A0 (Hewlett Packard)
Nmap scan report for npic3f08e.fim.uni-linz.ac.at (140.78.100.138)
Host is up (0.0020s latency).
MAC Address: 00:30:C1:C3:F0:8E (Hewlett-packard)
Nmap scan report for hpljm602.fim.uni-linz.ac.at (140.78.100.140)
Host is up (0.00s latency).
MAC Address: 2C:76:8A:3E:A0:E2 (Unknown)
Nmap scan report for praher-vista32.fim.uni-linz.ac.at (140.78.100.162)
Host is up (0.00s latency).
MAC Address: 00:1C:C0:1B:4A:F8 (Intel Corporate)
Nmap scan report for inge_xp.ads2-fim.fim.uni-linz.ac.at (140.78.100.165)
Host is up (0.0010s latency).
MAC Address: 00:1C:C0:32:C9:3C (Intel Corporate)
Nmap scan report for 140.78.100.168
Host is up (0.0030s latency).
MAC Address: 00:18:FE:D0:EA:40 (Hewlett Packard)
Nmap scan report for sabine-win7.ads2-fim.fim.uni-linz.ac.at (140.78.100.205)
Host is up (0.00s latency).
MAC Address: E0:69:95:4F:F7:03 (Unknown)
Nmap scan report for 140.78.100.206
Host is up (0.00s latency).
MAC Address: 00:22:15:A9:DD:A1 (Asustek Computer)
Nmap scan report for 140.78.100.208
Host is up (0.00s latency).
MAC Address: 40:6C:8F:46:EB:48 (Unknown)
Nmap scan report for michael_w7.ads2-fim.fim.uni-linz.ac.at (140.78.100.211)
Host is up.
Nmap scan report for jrm_win7.ads2-fim.fim.uni-linz.ac.at (140.78.100.212)
Host is up (0.00s latency).
MAC Address: E0:69:95:12:CD:15 (Unknown)
Nmap scan report for 140.78.100.250
Host is up (0.0030s latency).
MAC Address: 00:04:23:D3:FB:5C (Intel)
Nmap scan report for 140.78.100.251
Host is up (0.00s latency).
MAC Address: 00:04:23:D3:FB:5A (Intel)
Nmap done: 128 IP addresses (14 hosts up) scanned in 2.73 seconds
```

# Sample result: NMap info



# Sample result: NMap info



# Sample result: NMap info

Zenmap

Scan Werkzeuge Profil Hilfe

Ziel: 140.78.100.31 Profil: Comprehensive Scan Abbrechen

Befehl: nmap -sS -sU -sV -T4 -O -A -v -PE -PM -PP -PS -PA -PU -PO -PY 140.78.100.31

Rechner Dienste

Betriebssystem | Rechner

router.fi
r1-intern
hp2626-
hp2824-
hp2824-
hplj4100
npi8054
jrm_w7.
habib.fin
alex_v6
hoer_xp
alex_w2
cs140-7
fim_mac
praher-v
son_vist
140.78.
inge_sta

Nmap-Ausgabe | Ports / Rechner | Netzstruktur | Rechner-Details | Scans

nmap -sS -sU -sV -T4 -O -A -v -PE -PM -PP -PS -PA -PU -PO -PY 140.78.100.31 Details

```
Discovered open port 161/udp on 140.78.100.31
Completed UDP Scan at 15:21, 814.93s elapsed (1000 total ports)
Initiating Service scan at 15:21
Scanning 5 services on router.fim.uni-linz.ac.at (140.78.100.31)
Service scan Timing: About 60.00% done; ETC: 15:23 (0:00:51 remaining)
Completed Service scan at 15:22, 77.51s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against router.fim.uni-linz.ac.at (140.78.100.31)
Initiating Traceroute at 15:22
Completed Traceroute at 15:22, 0.01s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 15:22
Completed Parallel DNS resolution of 2 hosts. at 15:22, 0.00s elapsed
NSE: Script scanning 140.78.100.31.
Initiating NSE at 15:22
Completed NSE at 15:23, 5.01s elapsed
Nmap scan report for router.fim.uni-linz.ac.at (140.78.100.31)
Host is up (0.00024s latency).
Not shown: 1984 closed ports
PORT      STATE         SERVICE        VERSION
135/tcp   filtered      msrpc
139/tcp   filtered      netbios-ssn
445/tcp   filtered      microsoft-ds
593/tcp   filtered      http-rpc-epmap
1434/tcp  filtered      ms-sql-m
67/udp    open|filtered dhcps
123/udp   open          ntp            NTP v4
| ntp-info:
|   receive time stamp: 05/17/11 15:23:01
|   system: cisco
|   leap: 0
```

# Sample result: NMap info

```
1434/tcp  filtered      ms-sql-m
67/udp    open|filtered dhcps
123/udp   open          ntp            NTP v4
| ntp-info:
|   receive time stamp: 05/17/11 15:23:01
|   system: cisco
|   leap: 0
|   stratum: 4
|   rootdelay: 4.33
|   rootdispersion: 49.09
|   peer: 34814
|   refid: 140.78.2.62
|   reftime: 0xD17CF524.E5B5F39E
|   poll: 6
|   clock: 0xD17CF531.5D3A7B03
|   phase: 0.212
|   freq: 28.90
|_  error: 0.03
135/udp   filtered      msrpc
136/udp   filtered      profile
137/udp   filtered      netbios-ns
138/udp   filtered      netbios-dgm
139/udp   filtered      netbios-ssn
161/udp   open          snmp           Cisco SNMP service
|_snmp-win32-shares: TIMEOUT
162/udp   open|filtered snmptrap
1434/udp  filtered      ms-sql-m
10000/udp open|filtered ndmp
Device type: router|switch
Running: Cisco IOS 12.X
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

TRACEROUTE (using port 8888/tcp)
HOP RTT     ADDRESS
1   1.00 ms r1-intern.fim.uni-linz.ac.at (140.78.100.129)
2   1.00 ms router.fim.uni-linz.ac.at (140.78.100.31)

Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 909.68 seconds
           Raw packets sent: 2296 (84.307KB) | Rcvd: 2040 (98.464KB)
```

Filtere Rechner

# 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!
- Access:
  - → Google search
  - → Directly: “cache: <URL>”
    - » E.g. “cache:www.jku.at”

# 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!

# Common display filtering expressions (1)

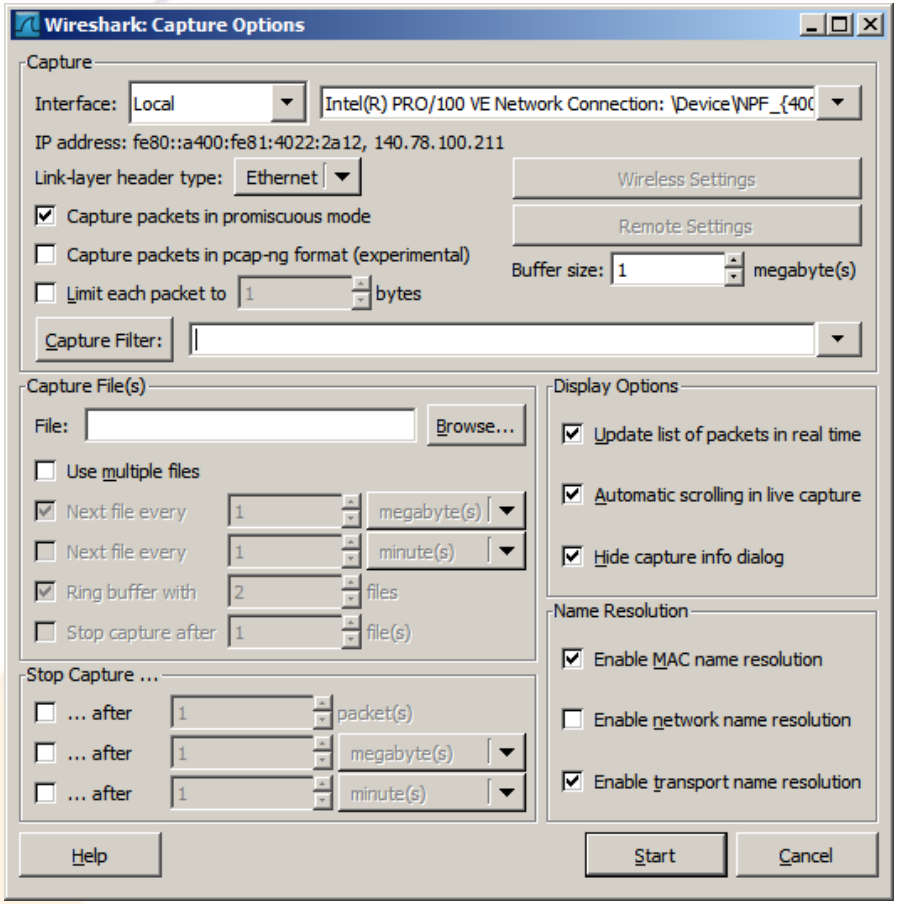
- Operators: == != < > <= >= && || ^^ !
  - → […] or […:…] or […-…]: Offset / Offset:Length / Offset-End
    - » Only possible as comparison, e.g. eth.src[0:3]==08:15:47!
- Layer 1/2: frame.??? / eth.???, arp.???, ppp.???
  - → Usually not very interesting
- Layer 3: ip.???, ipv6.???, icmp.???, icmpv6.???
  - → 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

See also: http://packetlife.net/library/cheat-sheets/

# 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

Intel(R) PRO/100 VE Network Connection - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | Intel_76:be:36 | Broadcast | ARP | Who has 140.78.100.141? Tell 140.78.100.174 |
| 2 | 0.174052 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 3 | 0.579412 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |
| 4 | 0.864438 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 5 | 0.999988 | Intel_76:be:36 | Broadcast | ARP | Who has 140.78.100.141? Tell 140.78.100.174 |
| 6 | 1.854523 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 7 | 2.158932 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 8 | 2.160081 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 9 | 2.579815 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |
| 10 | 2.854583 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 11 | 3.149568 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 12 | 3.150553 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 13 | 4.149606 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 14 | 4.150692 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 15 | 4.331539 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 16 | 4.580183 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |
| 17 | 5.149709 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 18 | 5.151104 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 19 | 5.174213 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 20 | 6.174206 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 21 | 6.590423 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |

```
⊟ Frame 8 (74 bytes on wire, 74 bytes captured)
    Arrival Time: May 18, 2012 13:02:17.726145000
    [Time delta from previous captured frame: 0.001149000 seconds]
    [Time delta from previous displayed frame: 0.001149000 seconds]
    [Time since reference or first frame: 2.160081000 seconds]
    Frame Number: 8
    Frame Length: 74 bytes
    Capture Length: 74 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
⊞ Ethernet II, Src: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2), Dst: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f)
⊞ Internet Protocol, Src: 140.78.100.140 (140.78.100.140), Dst: 140.78.100.211 (140.78.100.211)
⊞ Internet Control Message Protocol
```

```
0000  00 13 20 e9 2d 7f 2c 76  8a 3e a0 e2 08 00 45 00   .. .-.,v .>....E.
0010  00 3c 0a 5c 00 00 40 01  8e 69 8c 4e 64 8c 8c 4e   .<.\..@. .i.Nd..N
0020  64 d3 00 00 55 40 00 01  00 1b 61 62 63 64 65 66   d...U@.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

File: "C:\Users\michael\AppData\Local\Temp\wir... | Packets: 21 Displayed: 21 Marked: 0 Dropped: 0 | Profile: Default

# Wireshark Ping

Intel(R) PRO/100 VE Network Connection - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | Intel_76:be:36 | Broadcast | ARP | Who has 140.78.100.141? Tell 140.78.100.174 |
| 2 | 0.174052 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 3 | 0.579412 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |
| 4 | 0.864438 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 5 | 0.999988 | Intel_76:be:36 | Broadcast | ARP | Who has 140.78.100.141? Tell 140.78.100.174 |
| 6 | 1.854523 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 7 | 2.158932 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 8 | 2.160081 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 9 | 2.579815 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |
| 10 | 2.854583 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 11 | 3.149568 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 12 | 3.150553 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 13 | 4.149606 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 14 | 4.150692 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 15 | 4.331539 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 16 | 4.580183 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |
| 17 | 5.149709 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 18 | 5.151104 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 19 | 5.174213 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 20 | 6.174206 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 21 | 6.590423 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |

```
⊞ Frame 8 (74 bytes on wire, 74 bytes captured)
⊟ Ethernet II, Src: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2), Dst: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f)
  ⊟ Destination: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f)
      Address: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2)
      Address: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 140.78.100.140 (140.78.100.140), Dst: 140.78.100.211 (140.78.100.211)
⊞ Internet Control Message Protocol
```

```
0000  00 13 20 e9 2d 7f 2c 76  8a 3e a0 e2 08 00 45 00   .. .-.,v .>....E.
0010  00 3c 0a 5c 00 00 40 01  8e 69 8c 4e 64 8c 8c 4e   .<.\..@. .i.Nd..N
0020  64 d3 00 00 55 40 00 01  00 1b 61 62 63 64 65 66   d...U@.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Source Hardware Address (eth.src), 6 bytes | Packets: 21 Displayed: 21 Marked: 0 Dropped: 0 | Profile: Default

# Wireshark Ping

Intel(R) PRO/100 VE Network Connection - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | Intel_76:be:36 | Broadcast | ARP | Who has 140.78.100.141? Tell 140.78.100.174 |
| 2 | 0.174052 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 3 | 0.579412 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |
| 4 | 0.864438 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 5 | 0.999988 | Intel_76:be:36 | Broadcast | ARP | Who has 140.78.100.141? Tell 140.78.100.174 |
| 6 | 1.854523 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 7 | 2.158932 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 8 | 2.160081 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 9 | 2.579815 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |
| 10 | 2.854583 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 11 | 3.149568 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 12 | 3.150553 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 13 | 4.149606 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 14 | 4.150692 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 15 | 4.331539 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 16 | 4.580183 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |
| 17 | 5.149709 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 18 | 5.151104 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 19 | 5.174213 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 20 | 6.174206 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 21 | 6.590423 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |

```
⊞ Frame 8 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2), Dst: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f)
⊟ Internet Protocol, Src: 140.78.100.140 (140.78.100.140), Dst: 140.78.100.211 (140.78.100.211)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 60
    Identification: 0x0a5c (2652)
  ⊟ Flags: 0x00
      0.. = Reserved bit: Not Set
      .0. = Don't fragment: Not Set
      ..0 = More fragments: Not Set
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (0x01)
  ⊞ Header checksum: 0x8e69 [correct]
    Source: 140.78.100.140 (140.78.100.140)
    Destination: 140.78.100.211 (140.78.100.211)
⊞ Internet Control Message Protocol
```

```
0000  00 13 20 e9 2d 7f 2c 76  8a 3e a0 e2 08 00 45 00   .. .-.,v .>....E.
0010  00 3c 0a 5c 00 00 40 01  8e 69 8c 4e 64 8c 8c 4e   .<.\..@. .i.Nd..N
0020  64 d3 00 00 55 40 00 01  00 1b 61 62 63 64 65 66   d...U@.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Flags (ip.flags), 1 byte | Packets: 21 Displayed: 21 Marked: 0 Dropped: 0 | Profile: Default

# Wireshark Ping

Intel(R) PRO/100 VE Network Connection - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | Intel_76:be:36 | Broadcast | ARP | Who has 140.78.100.141? Tell 140.78.100.174 |
| 2 | 0.174052 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 3 | 0.579412 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |
| 4 | 0.864438 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 5 | 0.999988 | Intel_76:be:36 | Broadcast | ARP | Who has 140.78.100.141? Tell 140.78.100.174 |
| 6 | 1.854523 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 7 | 2.158932 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 8 | 2.160081 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 9 | 2.579815 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |
| 10 | 2.854583 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 11 | 3.149568 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 12 | 3.150553 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 13 | 4.149606 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 14 | 4.150692 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 15 | 4.331539 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 16 | 4.580183 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |
| 17 | 5.149709 | 140.78.100.211 | 140.78.100.140 | ICMP | Echo (ping) request |
| 18 | 5.151104 | 140.78.100.140 | 140.78.100.211 | ICMP | Echo (ping) reply |
| 19 | 5.174213 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 20 | 6.174206 | e0:69:95:12:cd:15 | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.212 |
| 21 | 6.590423 | HewlettP_c9:64:72 | Spanning-tree-(for-br | STP | RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e |

```
⊞ Frame 8 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2), Dst: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f)
⊞ Internet Protocol, Src: 140.78.100.140 (140.78.100.140), Dst: 140.78.100.211 (140.78.100.211)
⊟ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0 ()
    Checksum: 0x5540 [correct]
    Identifier: 0x0001
    Sequence number: 27 (0x001b)
  ⊟ Data (32 bytes)
      Data: 6162636465666768696A6B6C6D6E6F707172737475767761...
      [Length: 32]
```

```
0000  00 13 20 e9 2d 7f 2c 76  8a 3e a0 e2 08 00 45 00   .. .-.,v .>....E.
0010  00 3c 0a 5c 00 00 40 01  8e 69 8c 4e 64 8c 8c 4e   .<.\..@. .i.Nd..N
0020  64 d3 00 00 55 40 00 01  00 1b 61 62 63 64 65 66   d...U@.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Data (data.data), 32 bytes | Packets: 21 Displayed: 21 Marked: 0 Dropped: 0 | Profile: Default

# Wireshark
# HTTP - DNS

Intel(R) PRO/100 VE Network Connection - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

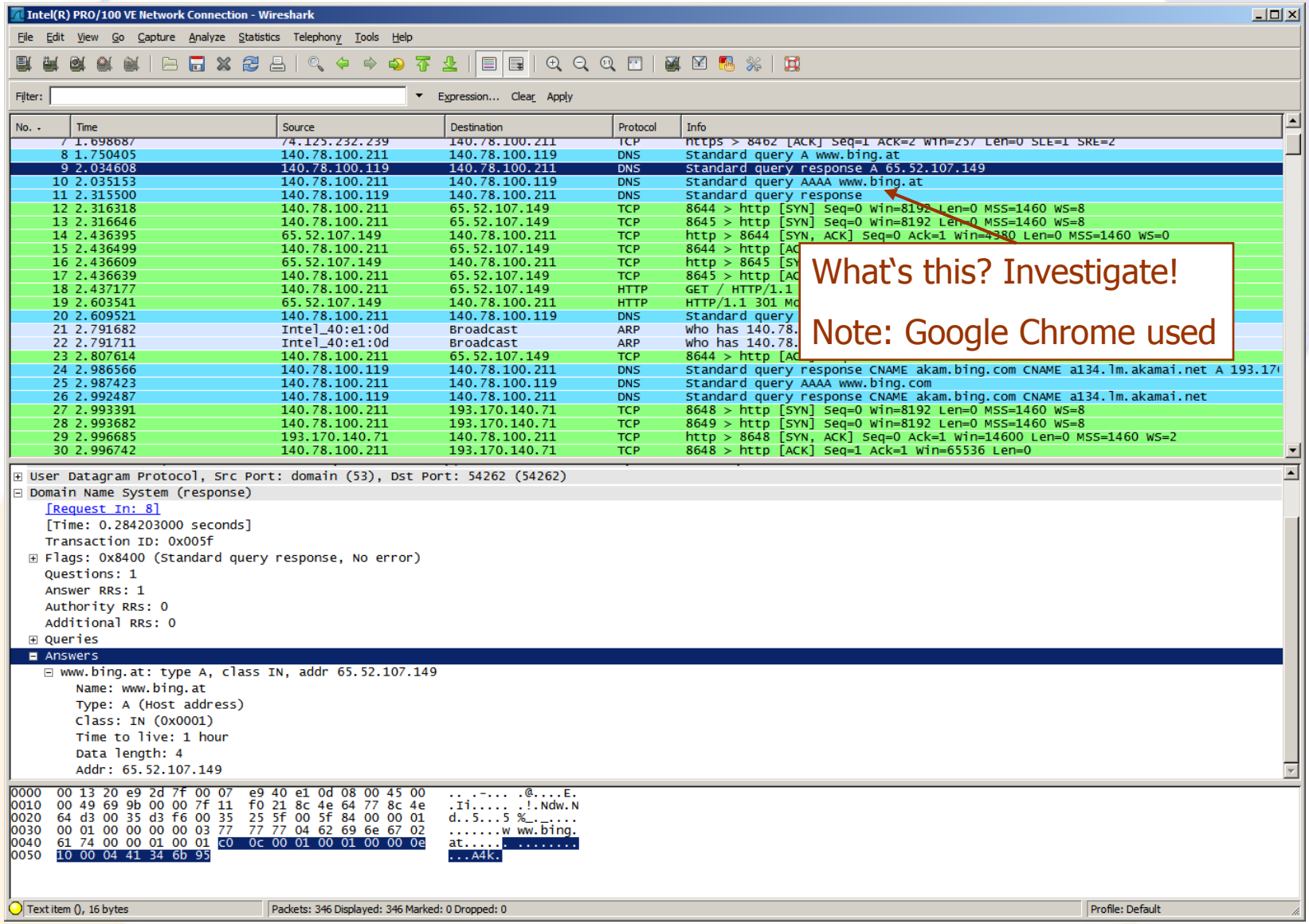
| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 7 | 1.698687 | 74.125.232.239 | 140.78.100.211 | TCP | https > 8462 [ACK] Seq=1 Ack=2 Win=257 Len=0 SLE=1 SRE=2 |
| 8 | 1.750405 | 140.78.100.211 | 140.78.100.119 | DNS | Standard query A www.bing.at |
| 9 | 2.034608 | 140.78.100.119 | 140.78.100.211 | DNS | Standard query response A 65.52.107.149 |
| 10 | 2.035153 | 140.78.100.211 | 140.78.100.119 | DNS | Standard query AAAA www.bing.at |
| 11 | 2.315500 | 140.78.100.119 | 140.78.100.211 | DNS | Standard query response |
| 12 | 2.316318 | 140.78.100.211 | 65.52.107.149 | TCP | 8644 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 |
| 13 | 2.316646 | 140.78.100.211 | 65.52.107.149 | TCP | 8645 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 |
| 14 | 2.436395 | 65.52.107.149 | 140.78.100.211 | TCP | http > 8644 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=0 |
| 15 | 2.436499 | 140.78.100.211 | 65.52.107.149 | TCP | 8644 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 16 | 2.436609 | 65.52.107.149 | 140.78.100.211 | TCP | http > 8645 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=0 |
| 17 | 2.436639 | 140.78.100.211 | 65.52.107.149 | TCP | 8645 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 18 | 2.437177 | 140.78.100.211 | 65.52.107.149 | HTTP | GET / HTTP/1.1 |
| 19 | 2.603541 | 65.52.107.149 | 140.78.100.211 | HTTP | HTTP/1.1 301 Moved Permanently |
| 20 | 2.609521 | 140.78.100.211 | 140.78.100.119 | DNS | Standard query A www.bing.com |
| 21 | 2.791682 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.141? Tell 140.78.100.129 |
| 22 | 2.791711 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell 140.78.100.129 |
| 23 | 2.807614 | 140.78.100.211 | 65.52.107.149 | TCP | 8644 > http [ACK] Seq=396 Ack=302 Win=65280 Len=0 |
| 24 | 2.986566 | 140.78.100.119 | 140.78.100.211 | DNS | Standard query response CNAME akam.bing.com CNAME a134.lm.akamai.net A 193.17 |
| 25 | 2.987423 | 140.78.100.211 | 140.78.100.119 | DNS | Standard query AAAA www.bing.com |
| 26 | 2.992487 | 140.78.100.119 | 140.78.100.211 | DNS | Standard query response CNAME akam.bing.com CNAME a134.lm.akamai.net |
| 27 | 2.993391 | 140.78.100.211 | 193.170.140.71 | TCP | 8648 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 |
| 28 | 2.993682 | 140.78.100.211 | 193.170.140.71 | TCP | 8649 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 |
| 29 | 2.996685 | 193.170.140.71 | 140.78.100.211 | TCP | http > 8648 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=2 |
| 30 | 2.996742 | 140.78.100.211 | 193.170.140.71 | TCP | 8648 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0 |

```
⊞ Frame 8 (71 bytes on wire, 71 bytes captured)
⊞ Ethernet II, Src: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f), Dst: Intel_40:e1:0d (00:07:e9:40:e1:0d)
⊞ Internet Protocol, Src: 140.78.100.211 (140.78.100.211), Dst: 140.78.100.119 (140.78.100.119)
⊞ User Datagram Protocol, Src Port: 54262 (54262), Dst Port: domain (53)
⊟ Domain Name System (query)
    [Response In: 9]
    Transaction ID: 0x005f
  ⊞ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.bing.at: type A, class IN
        Name: www.bing.at
        Type: A (Host address)
        Class: IN (0x0001)
```

```
0000  00 07 e9 40 e1 0d 00 13  20 e9 2d 7f 08 00 45 00   ...@....  .-...E.
0010  00 39 2b 6b 00 00 80 11  2d 62 8c 4e 64 d3 8c 4e   .9+k.... -b.Nd..N
0020  64 77 d3 f6 00 35 00 25  94 fb 00 5f 01 00 00 01   dw...5.% ..._....
0030  00 00 00 00 00 00 03 77  77 77 04 62 69 6e 67 02   .......w ww.bing.
0040  61 74 00 00 01 00 01                               at.....
```

Text item (), 17 bytes | Packets: 346 Displayed: 346 Marked: 0 Dropped: 0 | Profile: Default

# Wireshark
# HTTP - DNS



# Wireshark
# HTTP - Request

Intel(R) PRO/100 VE Network Connection - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 11 | 2.315500 | 140.78.100.119 | 140.78.100.211 | DNS | Standard query response |
| 12 | 2.316318 | 140.78.100.211 | 65.52.107.149 | TCP | 8644 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 |
| 13 | 2.316646 | 140.78.100.211 | 65.52.107.149 | TCP | 8645 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 |
| 14 | 2.436395 | 65.52.107.149 | 140.78.100.211 | TCP | http > 8644 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=0 |
| 15 | 2.436499 | 140.78.100.211 | 65.52.107.149 | TCP | 8644 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 16 | 2.436609 | 65.52.107.149 | 140.78.100.211 | TCP | http > 8645 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=0 |
| 17 | 2.436639 | 140.78.100.211 | 65.52.107.149 | TCP | 8645 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 18 | 2.437177 | 140.78.100.211 | 65.52.107.149 | HTTP | GET / HTTP/1.1 |
| 19 | 2.603541 | 65.52.107.149 | 140.78.100.211 | HTTP | HTTP/1.1 301 Moved Permanently |
| 20 | 2.609521 | 140.78.100.211 | 140.78.100.119 | DNS | Standard query A www.bing.com |
| 21 | 2.791682 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.141? Tell |
| 22 | 2.791711 | Intel_40:e1:0d | Broadcast | ARP | Who has 140.78.100.138? Tell |

What are these? Investigate!

```
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: www.bing.at\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.168 Safari/535.19\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Encoding: gzip,deflate,sdch\r\n
    Accept-Language: de-DE,de;q=0.8,en-US;q=0.6,en;q=0.4\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n
    \r\n
```

```
0010  01 b3 2b 71 40 00 80 06  2f e9 8c 4e 64 d3 41 34   ..+q@... /..Nd.A4
0020  6b 95 21 c4 00 50 b7 fd  f0 00 b8 d9 50 cc 50 18   k.!..P.. ....P.P.
0030  01 00 89 08 00 00 47 45  54 20 2f 20 48 54 54 50   ......GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  62 69 6e 67 2e 61 74 0d  0a 43 6f 6e 6e 65 63 74   bing.at. .Connect
0060  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69 76 65 0d   ion: kee p-alive.
0070  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   .User-Ag ent: Moz
0080  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
0090  73 20 4e 54 20 36 2e 31  3b 20 57 4f 57 36 34 29   s NT 6.1 ; WOW64)
00a0  20 41 70 70 6c 65 57 65  62 4b 69 74 2f 35 33 35    AppleWe bKit/535
00b0  2e 31 39 20 28 4b 48 54  4d 4c 2c 20 6c 69 6b 65   .19 (KHT ML, like
00c0  20 47 65 63 6b 6f 29 20  43 68 72 6f 6d 65 2f 31    Gecko)  Chrome/1
00d0  38 2e 30 2e 31 30 32 35  2e 31 36 38 20 53 61 66   8.0.1025 .168 Saf
00e0  61 72 69 2f 35 33 35 2e  31 39 0d 0a 41 63 63 65   ari/535. 19..Acce
00f0  70 74 3a 20 74 65 78 74  2f 68 74 6d 6c 2c 61 70   pt: text /html,ap
0100  70 6c 69 63 61 74 69 6f  6e 2f 78 68 74 6d 6c 2b   plicatio n/xhtml+
0110  78 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   xml,appl ication/
0120  78 6d 6c 3b 71 3d 30 2e  39 2c 2a 2f 2a 3b 71 3d   xml;q=0. 9,*/*;q=
0130  30 2e 38 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   0.8..Acc ept-Enco
0140  64 69 6e 67 3a 20 67 7a  69 70 2c 64 65 66 6c 61   ding: gz ip,defla
0150  74 65 2c 73 64 63 68 0d  0a 41 63 63 65 70 74 2d   te,sdch. .Accept-
0160  4c 61 6e 67 75 61 67 65  3a 20 64 65 2d 44 45 2c   Language : de-DE,
0170  64 65 3b 71 3d 30 2e 38  2c 65 6e 2d 55 53 3b 71   de;q=0.8 ,en-US;q
0180  3d 30 2e 36 2c 65 6e 3b  71 3d 30 2e 34 0d 0a 41   =0.6,en; q=0.4..A
0190  63 63 65 70 74 2d 43 68  61 72 73 65 74 3a 20 49   ccept-Ch arset: I
01a0  53 4f 2d 38 38 35 39 2d  31 2c 75 74 66 2d 38 3b   SO-8859- 1,utf-8;
01b0  71 3d 30 2e 37 2c 2a 3b  71 3d 30 2e 33 0d 0a 0d   q=0.7,*; q=0.3...
01c0  0a                                                 .
```

Hypertext Transfer Protocol (http), 395 bytes | Packets: 346 Displayed: 346 Marked: 0 Dropped: 0 | Profile: Default

# Wireshark
# HTTP - Response

Intel(R) PRO/100 VE Network Connection - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 13 | 2.316646 | 140.78.100.211 | 65.52.107.149 | TCP | 8645 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 |
| 14 | 2.436395 | 65.52.107.149 | 140.78.100.211 | TCP | http > 8644 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=0 |
| 15 | 2.436499 | 140.78.100.211 | 65.52.107.149 | TCP | 8644 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 16 | 2.436609 | 65.52.107.149 | 140.78.100.211 | TCP | http > 8645 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=0 |
| 17 | 2.436639 | 140.78.100.211 | 65.52.107.149 | TCP | 8645 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 18 | 2.437177 | 140.78.100.211 | 65.52.107.149 | HTTP | GET / HTTP/1.1 |
| 19 | 2.603541 | 65.52.107.149 | 140.78.100.211 | HTTP | HTTP/1.1 301 Moved Permanently |
| 20 | 2.609521 | 140.78.100.211 | 140.78.100.119 | DNS | Standard query A www.bing.com |
| 21 | 2.791682 | Intel_40:e1:0d | Broadcast | ARP | who has 140.78.100.141? Tell 140.78.100.129 |
| 22 | 2.791711 | Intel_40:e1:0d | Broadcast | ARP | who has 140.78.100.138? Tell 140.78.100.129 |
| 23 | 2.807614 | 140.78.100.211 | 65.52.107.149 | TCP | 8644 > http [ACK] Seq=396 Ack=302 Win=65280 Len=0 |
| 24 | 2.986566 | 140.78.100.119 | 140.78.100.211 | DNS | Standard query response CNAME akam.bing.com CNAME a134.lm.akamai.net A 193.17 |

```
⊞ Frame 19 (355 bytes on wire, 355 bytes captured)
⊞ Ethernet II, Src: Intel_40:e1:0d (00:07:e9:40:e1:0d), Dst: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f)
⊞ Internet Protocol, Src: 65.52.107.149 (65.52.107.149), Dst: 140.78.100.211 (140.78.100.211)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 8644 (8644), Seq: 1, Ack: 396, Len: 301
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 301 Moved Permanently\r\n
    ⊞ [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
      Request Version: HTTP/1.1
      Response Code: 301
    Cache-Control: no-cache\r\n
    Location: http://www.bing.com/?cc=at\r\n
    Edge-control: no-store\r\n
    P3P: CP="NON UNI COM NAV STA LOC CURa DEVa PSAa PSDa OUR IND"\r\n
    Set-Cookie: _HOP=I=1&TS=1337341091; domain=.bing.at; path=/\r\n
    Date: Fri, 18 May 2012 11:38:11 GMT\r\n
  ⊟ Content-Length: 0\r\n
      [Content length: 0]
    \r\n
```

Redirect

```
0010  01 55 8c 51 40 00 ee 06  61 66 41 34 6b 95 8c 4e   .U.Q@... afA4k..N
0020  64 d3 00 50 21 c4 b8 d9  50 cc b7 fd f1 8b 50 18   d..P!... P.....P.
0030  12 a7 88 5d 00 00 48 54  54 50 2f 31 2e 31 20 33   ...]..HT TP/1.1 3
0040  30 31 20 4d 6f 76 65 64  20 50 65 72 6d 61 6e 65   01 Moved  Permane
0050  6e 74 6c 79 0d 0a 43 61  63 68 65 2d 43 6f 6e 74   ntly..Ca che-Cont
0060  72 6f 6c 3a 20 6e 6f 2d  63 61 63 68 65 0d 0a 4c   rol: no- cache..L
0070  6f 63 61 74 69 6f 6e 3a  20 68 74 74 70 3a 2f 2f   ocation:  http://
0080  77 77 77 2e 62 69 6e 67  2e 63 6f 6d 2f 3f 63 63   www.bing .com/?cc
0090  3d 61 74 0d 0a 45 64 67  65 2d 63 6f 6e 74 72 6f   =at..Edg e-contro
00a0  6c 3a 20 6e 6f 2d 73 74  6f 72 65 0d 0a 50 33 50   l: no-st ore..P3P
00b0  3a 20 43 50 3d 22 4e 4f  4e 20 55 4e 49 20 43 4f   : CP="NO N UNI CO
00c0  4d 20 4e 41 56 20 53 54  41 20 4c 4f 43 20 43 55   M NAV ST A LOC CU
00d0  52 61 20 44 45 56 61 20  50 53 41 61 20 50 53 44   Ra DEVa  PSAa PSD
00e0  61 20 4f 55 52 20 49 4e  44 22 0d 0a 53 65 74 2d   a OUR IN D"..Set-
00f0  43 6f 6f 6b 69 65 3a 20  5f 48 4f 50 3d 49 3d 31   Cookie:  _HOP=I=1
0100  26 54 53 3d 31 33 33 37  33 34 31 30 39 31 3b 20   &TS=1337 341091;
0110  64 6f 6d 61 69 6e 3d 2e  62 69 6e 67 2e 61 74 3b   domain=. bing.at;
0120  20 70 61 74 68 3d 2f 0d  0a 44 61 74 65 3a 20 46    path=/. .Date: F
0130  72 69 2c 20 31 38 20 4d  61 79 20 32 30 31 32 20   ri, 18 M ay 2012
0140  31 31 3a 33 38 3a 31 31  20 47 4d 54 0d 0a 43 6f   11:38:11  GMT..Co
0150  6e 74 65 6e 74 2d 4c 65  6e 67 74 68 3a 20 30 0d   ntent-Le ngth: 0.
0160  0a 0d 0a                                           ...
```

HTTP Set Cookie (http.set_cookie), 61 bytes | Packets: 346 Displayed: 346 Marked: 0 Dropped: 0 | Profile: Default

P3P Compact Policy: http://www.p3pwriter.com/LRN_111.asp

# Wireshark
# HTTP - Stream

Follow TCP Stream

Stream Content

```
GET /?cc=at HTTP/1.1
Host: www.bing.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.168
Safari/535.19
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: de-DE,de;q=0.8,en-US;q=0.6,en;q=0.4
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Type: text/html; charset=utf-8
P3P: CP="NON UNI COM NAV STA LOC CURa DEVa PSAa PSDa OUR IND"
Vary: Accept-Encoding
Content-Encoding: gzip
Date: Fri, 18 May 2012 11:38:11 GMT
Content-Length: 10051
Connection: keep-alive
Set-Cookie: _FS=mkt=de-AT&NU=1; domain=.bing.com; path=/
Set-Cookie: _SS=SID=9C9E9DA7CB2B43F8B5832A8854ECF181; domain=.bing.com; path=/
Set-Cookie: MUID=264FA59BF1D561753F42A6FFF0D26193; expires=Sun, 18-May-2014 11:38:11 GMT; domain=.bing.com;
path=/
Set-Cookie: OrigMUID=264FA59BF1D561753F42A6FFF0D26193%2c5546792e35a8415997835740de96da67; expires=Sun, 18-
May-2014 11:38:11 GMT; domain=.bing.com; path=/
Set-Cookie: SRCHD=D=2303258&MS=2303258&AF=NOFORM; expires=Sun, 18-May-2014 11:38:11 GMT; domain=.bing.com; path=/
Set-Cookie: SRCHUID=V=2&GUID=EFF4F73D88574A12B17D3F6371AEC69D; expires=Sun, 18-May-2014 11:38:11 GMT; path=/
Set-Cookie: SRCHUSR=AUTOREDIR=0&GEOVAR=&DOB=20120518; expires=Sun, 18-May-2014 11:38:11 GMT; domain=.bing.com;
path=/

...........|.v.8...|......E....L.d.yq...N......HHb."..X..5g.b.....}..........@.......S.2...@ "..@.........^V....
\......B......f................b/.......oI...d9h6W...j.a4k..o~AX&6...Dj...KN.Y....,.RR...... ..@7..>.. ..../
hbW.0Hh.X$._.&~.V....4..d.8".....S..".z#y\Bo......eR.w....`.Rr.l.....=.y~./.7...........f......k.!8..lnM..A.
```

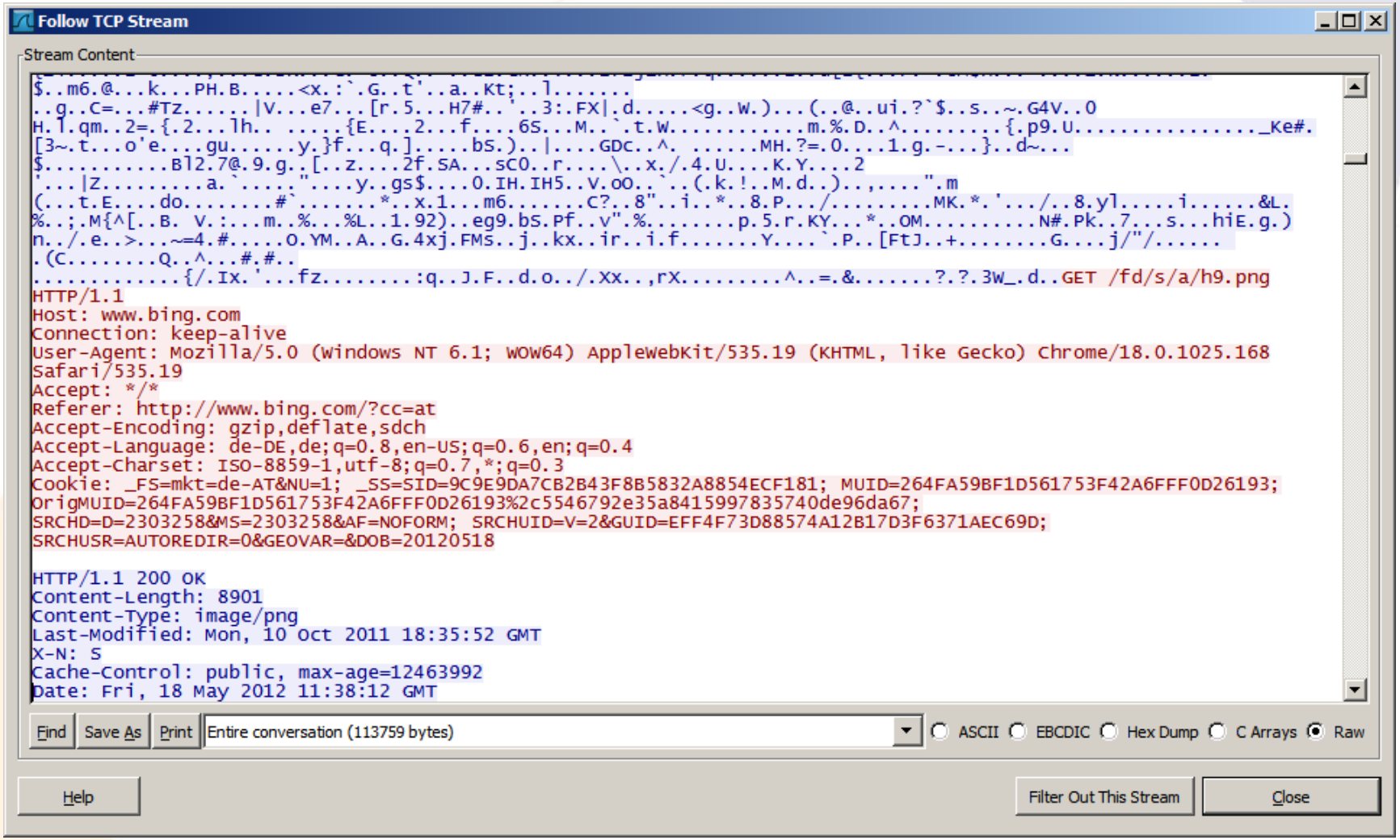
Find | Save As | Print | Entire conversation (113759 bytes) | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Help | Filter Out This Stream | Close

# 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

Intel(R) PRO/100 VE Network Connection - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: http  Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 13 | 6.804169 | 140.78.100.211 | 213.165.65.100 | HTTP | POST /de/cgi/login HTTP/1.1 (application/x-www-form-urlencoded) |
| 15 | 6.945697 | 213.165.65.100 | 140.78.100.211 | HTTP | HTTP/1.1 302 Found (text/html) |
| 19 | 6.985769 | 140.78.100.211 | 213.165.64.71 | HTTP | GET /?status=login-failed HTTP/1.1 |
| 21 | 7.019225 | 213.165.64.71 | 140.78.100.211 | HTTP | HTTP/1.1 301 Moved Permanently (text/html) |
| 25 | 7.058273 | 140.78.100.211 | 213.165.64.72 | HTTP | GET /?status=login-failed HTTP/1.1 |
| 42 | 7.180847 | 213.165.64.72 | 140.78.100.211 | HTTP | HTTP/1.1 200 OK (text/html) |
| 47 | 7.568014 | 140.78.100.211 | 213.165.64.72 | HTTP | GET /uim.html HTTP/1.1 |
| 50 | 7.597259 | 140.78.100.211 | 217.72.204.172 | HTTP | GET /ngvar.js HTTP/1.1 |
| 51 | 7.607270 | 213.165.64.72 | 140.78.100.211 | HTTP | HTTP/1.1 200 OK (text/html) |
| 52 | 7.623443 | 140.78.100.211 | 2.21.93.234 | HTTP | Continuation or non-HTTP traffic |
| 55 | 7.630422 | 217.72.204.172 | 140.78.100.211 | HTTP | HTTP/1.1 200 OK (application/x-javascript) |
| 64 | 7.831915 | 140.78.100.211 | 217.72.203.250 | HTTP | GET /?LogoutAdProxy.service=hpfirst&site=gmx&section=gmx/homepage/start/at/&c |

```
⊞ Frame 13 (754 bytes on wire, 754 bytes captured)
⊞ Ethernet II, Src: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f), Dst: Intel_40:e1:0d (00:07:e9:40:e1:0d)
⊞ Internet Protocol, Src: 140.78.100.211 (140.78.100.211), Dst: 213.165.65.100 (213.165.65.100)
⊞ Transmission Control Protocol, Src Port: 12107 (12107), Dst Port: http (80), Seq: 1, Ack: 1, Len: 700
⊟ Hypertext Transfer Protocol
  ⊟ POST /de/cgi/login HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): POST /de/cgi/login HTTP/1.1\r\n]
      Request Method: POST
      Request URI: /de/cgi/login
      Request Version: HTTP/1.1
    Host: service.gmx.net\r\n
    Connection: keep-alive\r\n
  ⊟ Content-Length: 116\r\n
      [Content length: 116]
    Cache-Control: max-age=0\r\n
    Origin: http://www.gmx.at\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.168 Safari/535.19\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Referer: http://www.gmx.at/?status=login-failed\r\n
    Accept-Encoding: gzip,deflate,sdch\r\n
    Accept-Language: de-DE,de;q=0.8,en-US;q=0.6,en;q=0.4\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n
    \r\n
⊟ Line-based text data: application/x-www-form-urlencoded
    AREA=1&EXT=redirect&EXT2=&dlevel=c&id=test%40gmx.at&p=password&jsenabled=true&uinguserid=ac14087b-27496-1337344698-6
```

```
0250  70 74 2d 43 68 61 72 73  65 74 3a 20 49 53 4f 2d   pt-Chars et: ISO-
0260  38 38 35 39 2d 31 2c 75  74 66 2d 38 3b 71 3d 30   8859-1,u tf-8;q=0
0270  2e 37 2c 2a 3b 71 3d 30  2e 33 0d 0a 0d 0a 41 52   .7,*;q=0 .3....AR
0280  45 41 3d 31 26 45 58 54  3d 72 65 64 69 72 65 63   EA=1&EXT =redirec
0290  74 26 45 58 54 32 3d 26  64 6c 65 76 65 6c 3d 63   t&EXT2=& dlevel=c
02a0  26 69 64 3d 74 65 73 74  25 34 30 67 6d 78 2e 61   &id=test %40gmx.a
02b0  74 26 70 3d 70 61 73 73  77 6f 72 64 26 6a 73 65   t&p=pass word&jse
02c0  6e 61 62 6c 65 64 3d 74  72 75 65 26 75 69 6e 67   nabled=t rue&uing
02d0  75 73 65 72 69 64 3d 61  63 31 34 30 38 37 62 2d   userid=a c14087b-
02e0  32 37 34 39 36 2d 31 33  33 37 33 34 34 36 39 38   27496-13 37344698
02f0  2d 36                                              -6
```

Text item (), 116 bytes | Packets: 323 Displayed: 46 Marked: 0 Dropped: 0 | Profile: Default

# Wireshark
# HTTP authentication + TLS

Intel(R) PRO/100 VE Network Connection - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: ssl || http  Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 20 | 1.708613 | 140.78.100.211 | 213.165.65.100 | TLSv1 | Client Hello |
| 22 | 1.765842 | 213.165.65.100 | 140.78.100.211 | TLSv1 | Server Hello, |
| 24 | 1.765849 | 213.165.65.100 | 140.78.100.211 | TLSv1 | Certificate, Server Key Exchange, Server Hello Done |
| 26 | 1.792478 | 140.78.100.211 | 213.165.65.100 | TLSv1 | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message, Applica |
| 27 | 1.834206 | 213.165.65.100 | 140.78.100.211 | TLSv1 | Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message |
| 28 | 1.892803 | 213.165.65.100 | 140.78.100.211 | TLSv1 | Application Data, Application Data |
| 37 | 1.983291 | 140.78.100.211 | 213.165.64.71 | HTTP | GET /?status=login-failed HTTP/1.1 |
| 39 | 2.016840 | 213.165.64.71 | 140.78.100.211 | HTTP | HTTP/1.1 301 Moved Permanently (text/html) |
| 47 | 2.118085 | 140.78.100.211 | 213.165.64.72 | HTTP | GET /?status=login-failed HTTP/1.1 |
| 62 | 2.242440 | 213.165.64.72 | 140.78.100.211 | HTTP | HTTP/1.1 200 OK (text/html) |
| 67 | 2.591299 | 140.78.100.211 | 213.165.64.72 | HTTP | GET /uim.html HTTP/1.1 |
| 70 | 2.618334 | 140.78.100.211 | 217.72.204.172 | HTTP | GET /novar.js HTTP/1.1 |

```
⊞ Frame 24 (991 bytes on wire, 991 bytes captured)
⊞ Ethernet II, Src: Intel_40:e1:0d (00:07:e9:40:e1:0d), Dst: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f)
⊞ Internet Protocol, Src: 213.165.65.100 (213.165.65.100), Dst: 140.78.100.211 (140.78.100.211)
⊞ Transmission Control Protocol, Src Port: https (443), Dst Port: 12203 (12203), Seq: 2921, Ack: 428, Len: 937
⊞ [Reassembled TCP Segments (3800 bytes): #22(1403), #23(1460), #24(937)]
⊟ Secure Socket Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 3256
    ⊟ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 3252
        Certificates Length: 3249
      ⊟ Certificates (3249 bytes)
          Certificate Length: 1007
        ⊞ Certificate (id-at-commonName=service.gmx.net,id-at-organizationalUnitName=GMX,id-at-organizationName=1&1 Mail & Media GmbH,id-at-localityName=Montabaur,id
          Certificate Length: 1136
        ⊞ Certificate (id-at-commonName=Thawte SSL CA,id-at-organizationName=Thawte, Inc.,id-at-countryName=US)
          Certificate Length: 1097
        ⊞ Certificate (id-at-commonName=thawte Primary Root CA,id-at-organizationalUnitName=(c) 2006 thawte, Inc. - For author,id-at-organizationalUnitName=Certifica
  ⊟ TLSv1 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 525
    ⊟ Handshake Protocol: Server Key Exchange
```

```
0000  00 13 20 e9 2d 7f 00 07  e9 40 e1 0d 08 00 45 00   .. .-... .@....E.
0010  03 d1 1d 6c 40 00 2d 06  24 90 d5 a5 41 64 8c 4e   ...l@.-. $...Ad.N
0020  64 d3 01 bb 2f ab 7e f8  12 e0 22 f1 ac 0f 50 18   d.../.~. ..".."..P.
0030  00 0e 7b ed 00 00 8c 9d  91 1f 97 6a 52 cb de 09   ..{..... ...jR...
0040  36 a4 77 d8 7b 87 50 44  d5 3e 6e 29 69 fb 39 49   6.w.{.PD .>n)i.9I
0050  26 1e 09 a5 80 7b 40 2d  eb e8 27 85 c9 fe 61 fd   &....{@- ..'...a.
0060  7e e6 7c 97 1d d5 9d 02  03 01 00 01 a3 81 c2 30   ~.|..... .......0
0070  81 bf 30 0f 06 03 55 1d  13 01 01 ff 04 05 30 03   ..0...U. ......0.
0080  01 01 ff 30 3b 06 03 55  1d 20 04 34 30 32 30 30   ...0;..U . .40200
0090  06 04 55 1d 20 00 30 28  30 26 06 08 2b 06 01 05   ..U. .0( 0&..+...
```

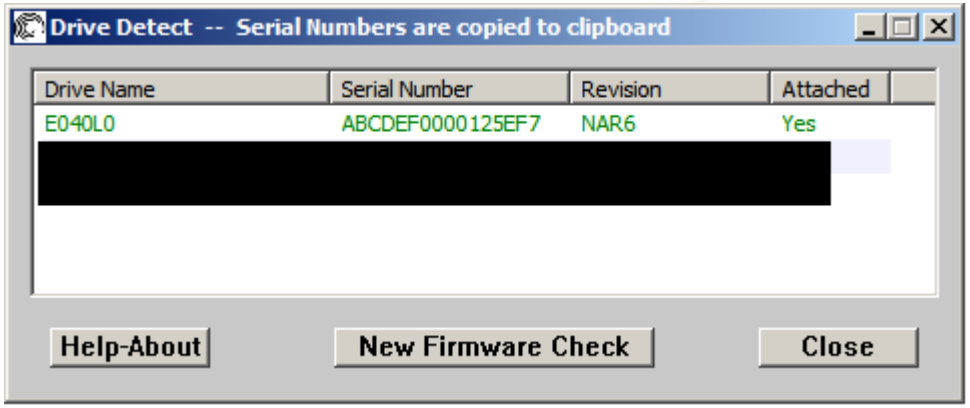
Frame (991 bytes) | Reassembled TCP (3800 bytes)

File: "C:\Users\michael\AppData\Local\Temp\wir... | Packets: 291 Displayed: 48 Marked: 0 Dropped: 0 | Profile: Default

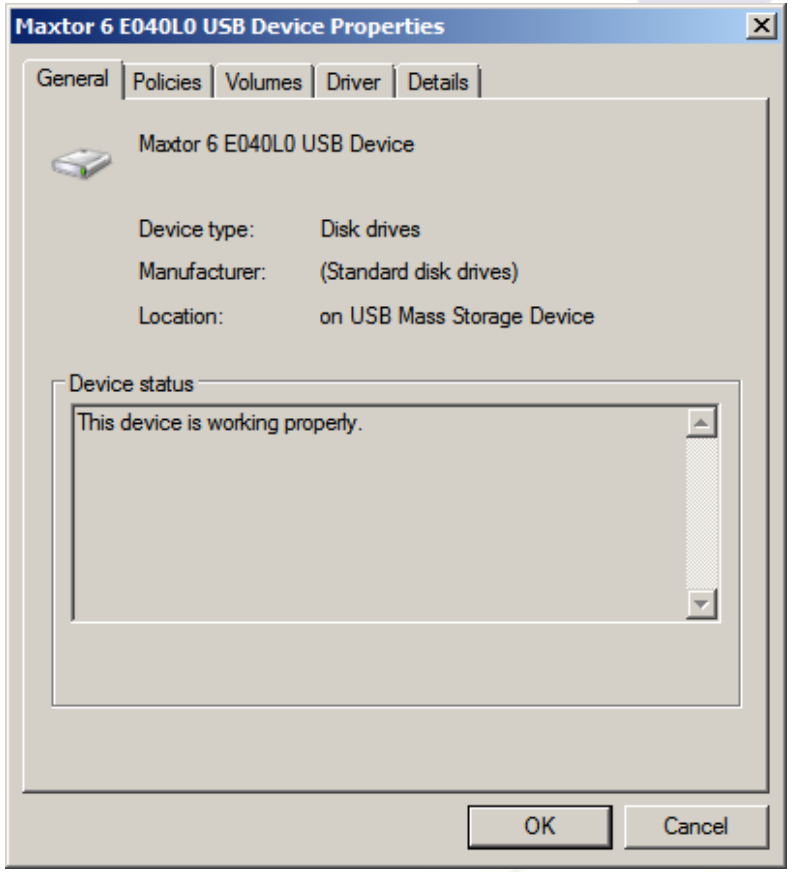
# Serial number: Photograph


- Code: NAR61HA0
- 6E040L0711214
- E1245D7N

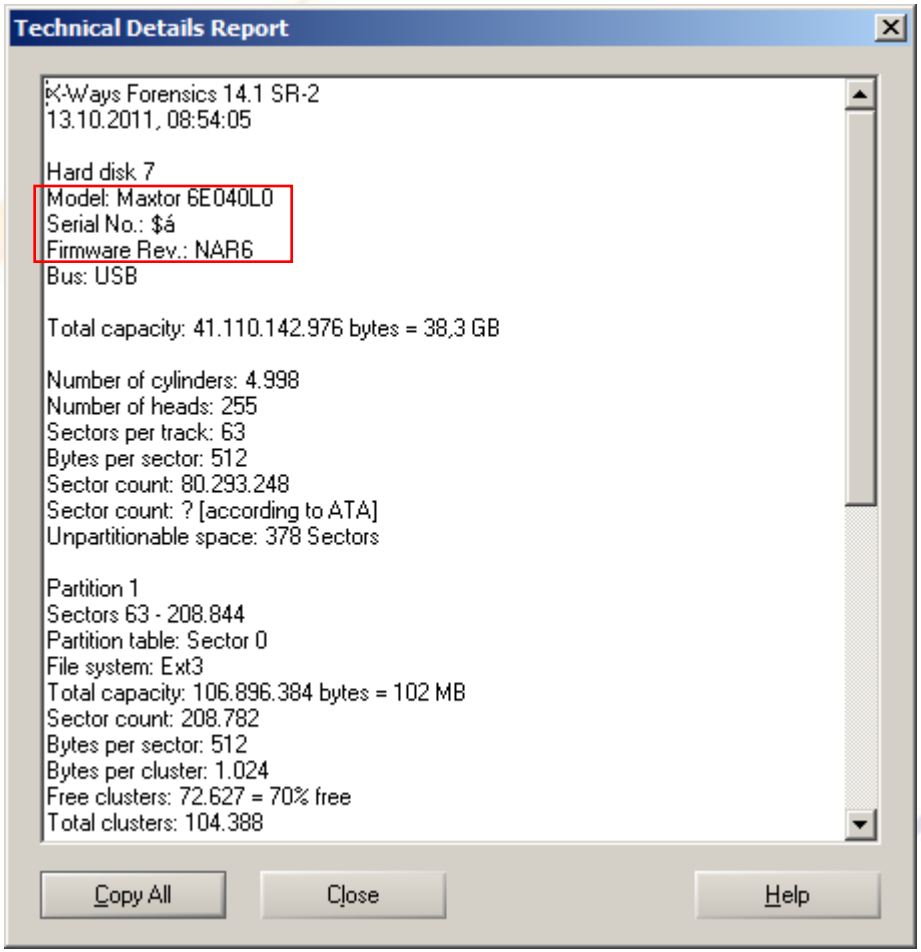
# Serial number: According to tools




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**

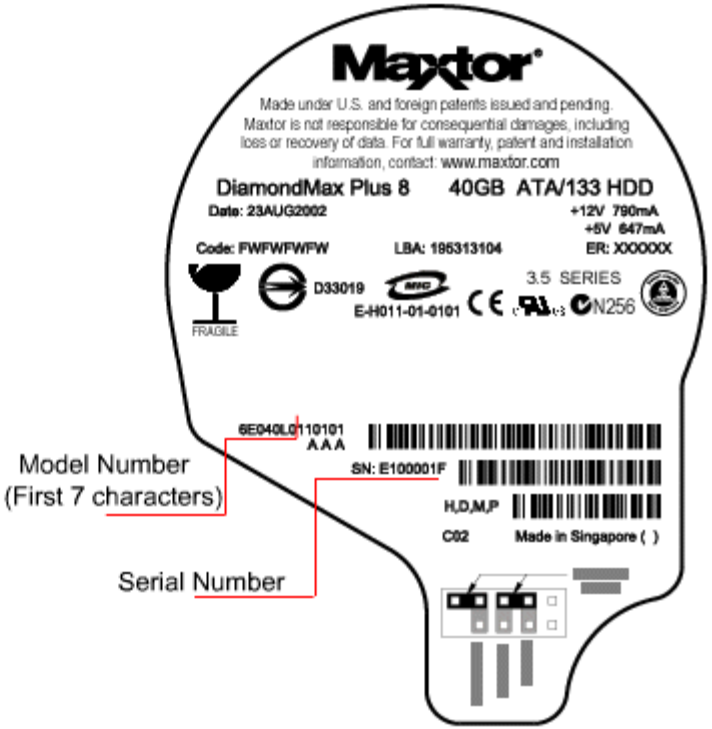
This label type can be found on the following Maxtor drive model:

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

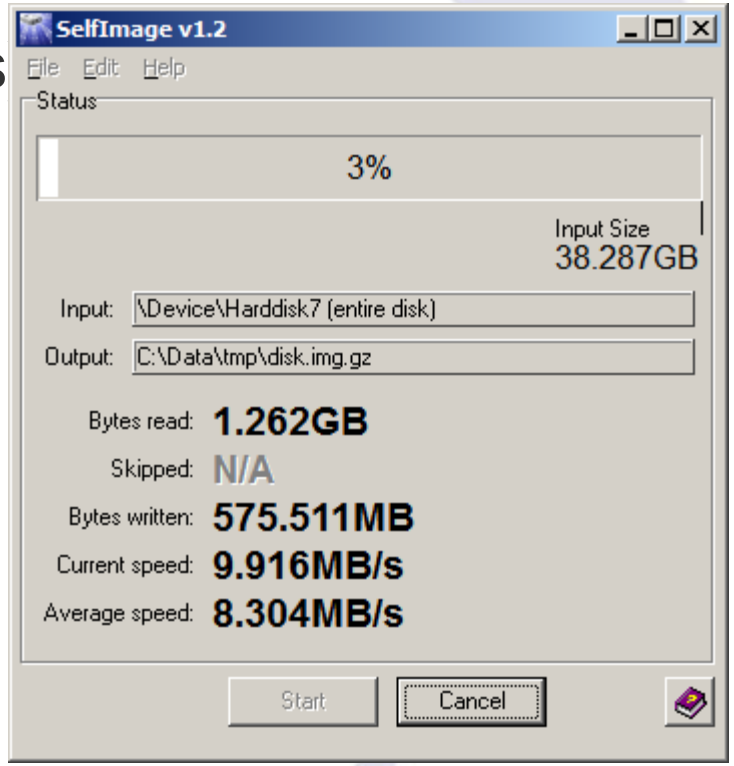


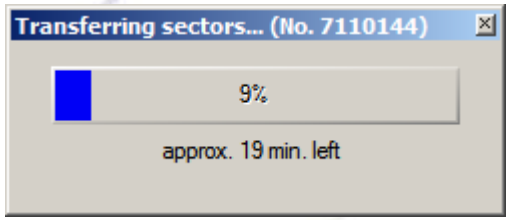

Main Menu | Print

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



# Disk image

- Variant D: OSFClone
  - → Self-booting (CD, USB, …)
  - → Free tool
  - → Formats: Raw, AFF
  - → http://www.osforensics.com/tools/create-disk-images.html
- Variant E: FTK Imager
  - → Free part of the commercial product “FTK”
    - » Installable version and portable one available
  - → Windows program
  - → Formats: Raw, AFF, Encase
  - → Supports also preview, obtaining copy of protected files (registry), …

# 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/