Collaborative Discussion 2 – Initial Post – Michael Geiger

During the practical activity in unit 3, I examined the website loadedwithstuff.co.uk. A Windows 10 OS was used for the tests and was carried out from Frankfurt, Germany.

The CMD command tracerout (tracert) was initially used to determine the number of hops and their delay from the source machine via the router to the website. This resulted in a total of 13 hops. For the determination of the greatest delay and its average time, however, this investigation method could not provide any significantly valid results, as only three tests are carried out with this tool and between hops 8 to 13 the delay in all hops was 15 ms to 18 ms and no average difference resulted in more than 2 ms.

In order to obtain a statistically more meaningful result, the WinMTR program from Appnor MSP was used. After 235 tests, hop 12 could be determined with an average delay of 26 ms and a longest delay of 199 ms. Even if the result is more informative, no statistical significance could be determined here either (p = 0.83).

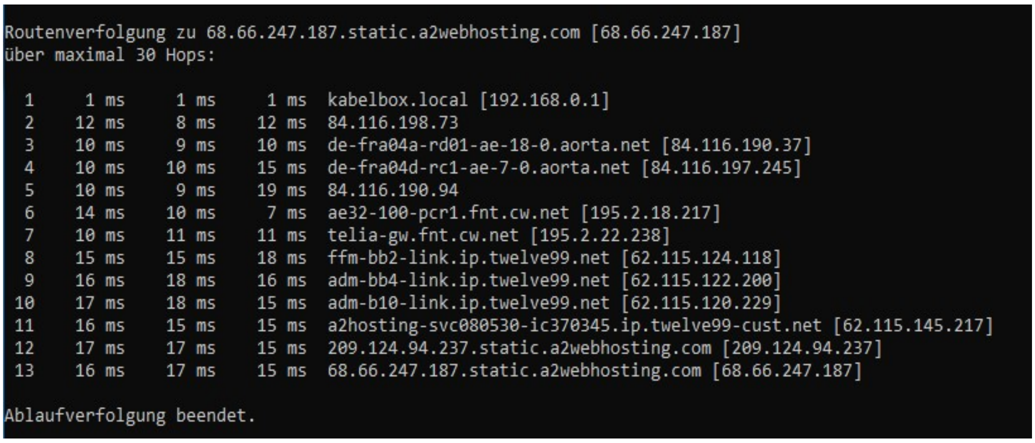
Since the tools required for further examinations are not preinstalled with the Windows 10 operating system, online applications were used for further examinations. With the help of the website dnstool.ch the main nameservers of the website loadedwithstuff.co.uk and the MX record could be determined. The main namservers are: ns1.a2hosting.com, ns2.a2hosting.com, ns3.a2hosting.com, ns4.a2hosting.com. The MX record from the website is: mail.loadedwithstuff.co.uk.

The who.is website was used to determine the registered contact. The research resulted in the organization A2 Hosting, Inc., based in Ann Arobr in Michigan, US.

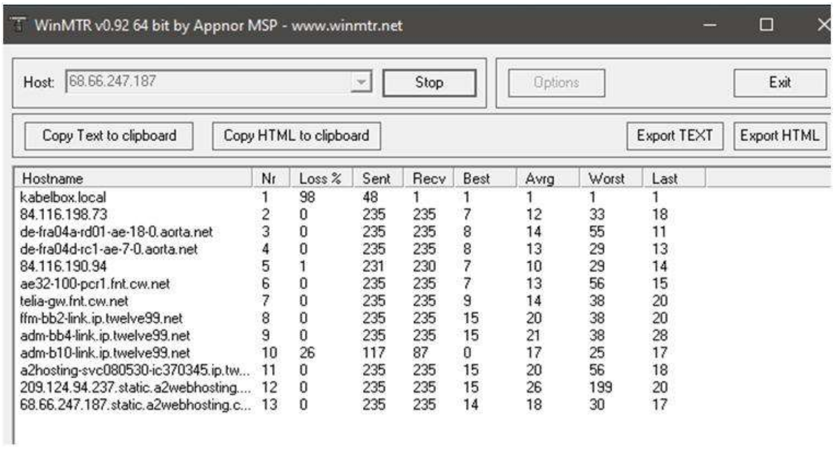
In order to find out where the website is hosted, a search was carried out on hostingchecker.com and the result was Amsterdam, Netherlands.

When carrying out the investigation, it became apparent that many of the necessary tools, such as nslookup, whois and dig, are not pre-installed under Windows 10. In order to obtain the results, online offers were used that carry out the analysis.

Screenshots of the information obtained from the respective tools or websites can be found below.

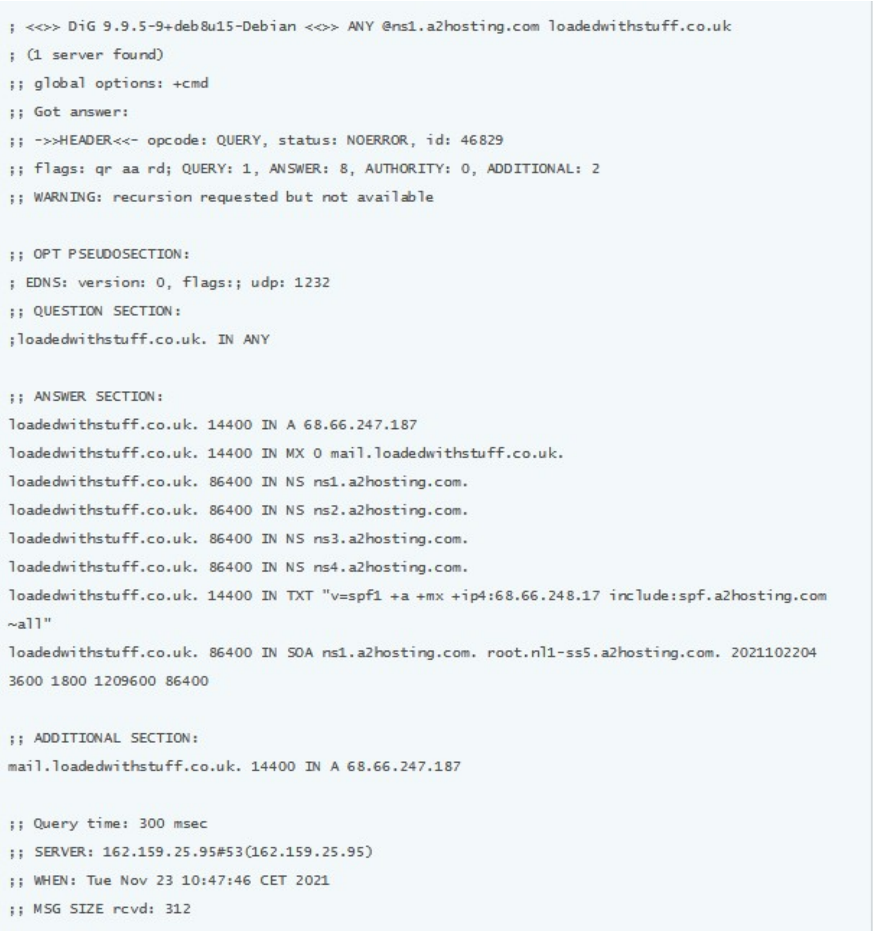


```
Routenverfolgung zu 68.66.247.187.static.a2webhosting.com [68.66.247.187]
über maximal 30 Hops:

  1     1 ms     1 ms     1 ms  kabelbox.local [192.168.0.1]
  2    12 ms     8 ms    12 ms  84.116.198.73
  3    10 ms     9 ms    10 ms  de-fra04a-rd01-ae-18-0.aorta.net [84.116.190.37]
  4    10 ms    10 ms    15 ms  de-fra04d-rc1-ae-7-0.aorta.net [84.116.197.245]
  5    10 ms     9 ms    19 ms  84.116.190.94
  6    14 ms    10 ms     7 ms  ae32-100-pcr1.fnt.cw.net [195.2.18.217]
  7    10 ms    11 ms    11 ms  telia-gw.fnt.cw.net [195.2.22.238]
  8    15 ms    15 ms    18 ms  ffm-bb2-link.ip.twelve99.net [62.115.124.118]
  9    16 ms    18 ms    16 ms  adm-bb4-link.ip.twelve99.net [62.115.122.200]
 10    17 ms    18 ms    15 ms  adm-b10-link.ip.twelve99.net [62.115.120.229]
 11    16 ms    15 ms    15 ms  a2hosting-svc080530-ic370345.ip.twelve99-cust.net [62.115.145.217]
 12    17 ms    17 ms    15 ms  209.124.94.237.static.a2webhosting.com [209.124.94.237]
 13    16 ms    17 ms    15 ms  68.66.247.187.static.a2webhosting.com [68.66.247.187]

Ablaufverfolgung beendet.
```

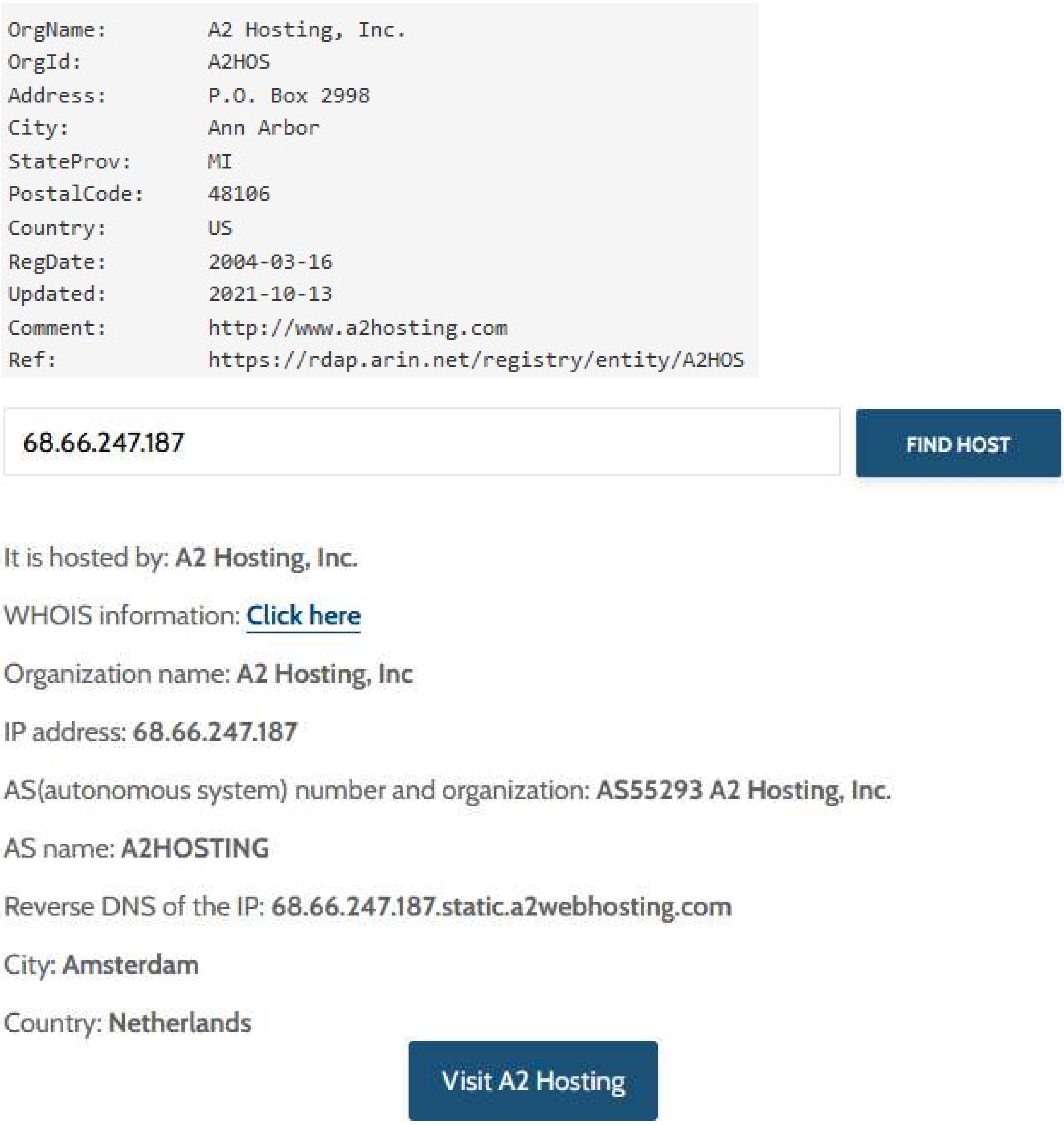


Host: 68.66.247.187

Hostname	Nr	Loss %	Sent	Recv	Best	Avrg	Worst	Last
kabelbox.local	1	98	48	1	1	1	1	1
84.116.198.73	2	0	235	235	7	12	33	18
de-fra04a-rd01-ae-18-0.aorta.net	3	0	235	235	8	14	55	11
de-fra04d-rc1-ae-7-0.aorta.net	4	0	235	235	8	13	29	13
84.116.190.94	5	1	231	230	7	10	29	14
ae32-100-pcr1.fnt.cw.net	6	0	235	235	7	13	56	15
telia-gw.fnt.cw.net	7	0	235	235	9	14	38	20
ffm-bb2-link.ip.twelve99.net	8	0	235	235	15	20	38	20
adm-bb4-link.ip.twelve99.net	9	0	235	235	15	21	38	28
adm-b10-link.ip.twelve99.net	10	26	117	87	0	17	25	17
a2hosting-svc080530-ic370345.ip.tw...	11	0	235	235	15	20	56	18
209.124.94.237.static.a2webhosting....	12	0	235	235	15	26	199	20
68.66.247.187.static.a2webhosting.c...	13	0	235	235	14	18	30	17



```
; <<>> DiG 9.9.5-9+deb8u15-Debian <<>> ANY @ns1.a2hosting.com loadedwithstuff.co.uk
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46829
;; flags: qr aa rd; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;loadedwithstuff.co.uk. IN ANY

;; ANSWER SECTION:
loadedwithstuff.co.uk. 14400 IN A 68.66.247.187
loadedwithstuff.co.uk. 14400 IN MX 0 mail.loadedwithstuff.co.uk.
loadedwithstuff.co.uk. 86400 IN NS ns1.a2hosting.com.
loadedwithstuff.co.uk. 86400 IN NS ns2.a2hosting.com.
loadedwithstuff.co.uk. 86400 IN NS ns3.a2hosting.com.
loadedwithstuff.co.uk. 86400 IN NS ns4.a2hosting.com.
loadedwithstuff.co.uk. 14400 IN TXT "v=spf1 +a +mx +ip4:68.66.248.17 include:spf.a2hosting.com
~all"
loadedwithstuff.co.uk. 86400 IN SOA ns1.a2hosting.com. root.nl1-ss5.a2hosting.com. 2021102204
3600 1800 1209600 86400

;; ADDITIONAL SECTION:
mail.loadedwithstuff.co.uk. 14400 IN A 68.66.247.187

;; Query time: 300 msec
;; SERVER: 162.159.25.95#53(162.159.25.95)
;; WHEN: Tue Nov 23 10:47:46 CET 2021
;; MSG SIZE rcvd: 312
```



```
OrgName:        A2 Hosting, Inc.
OrgId:          A2HOS
Address:        P.O. Box 2998
City:           Ann Arbor
StateProv:      MI
PostalCode:     48106
Country:        US
RegDate:        2004-03-16
Updated:        2021-10-13
Comment:        http://www.a2hosting.com
Ref:            https://rdap.arin.net/registry/entity/A2HOS
```

68.66.247.187

It is hosted by: **A2 Hosting, Inc.**

WHOIS information: **Click here**

Organization name: **A2 Hosting, Inc**

IP address: **68.66.247.187**

AS(autonomous system) number and organization: **AS55293 A2 Hosting, Inc.**

AS name: **A2HOSTING**

Reverse DNS of the IP: **68.66.247.187.static.a2webhosting.com**

City: **Amsterdam**

Country: **Netherlands**

References:

Hosting Checker (2021) Find out who is hosting any website. Available from: https://hostingchecker.com/ [Accessed:03.12.2021]

Sitepoint GmbH(2021) DNStools. Available from:http://www.dnstools.ch/dns-nameserver.html [Accessed: 03.12.2021]

Who.is (2021) WHOIS Search, Domain Name, Website, and IP Tools. Available from: https://who.is/whois-ip/ip-address/68.66.247.187 [Accessed: 03.12.2021]