Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Faculty of Computer Science

1st ITG Workshop on IT Security (ITSec)

Influence of HTTP Header Entries on the Forensic Analysis of Web Browser Artifacts

Tobias Scheible, M.Eng.

02.04.2020 Eberhard Karls Universität Tübingen

Outline

- Albstadt-Sigmaringen University
- Digital Forensics Investigation
- HTTP Header Entries
- Forensic Examination of Web Browser
- Influence on Web Browser Artefacts
- Conclusions and future work

Albstadt-Sigmaringen University

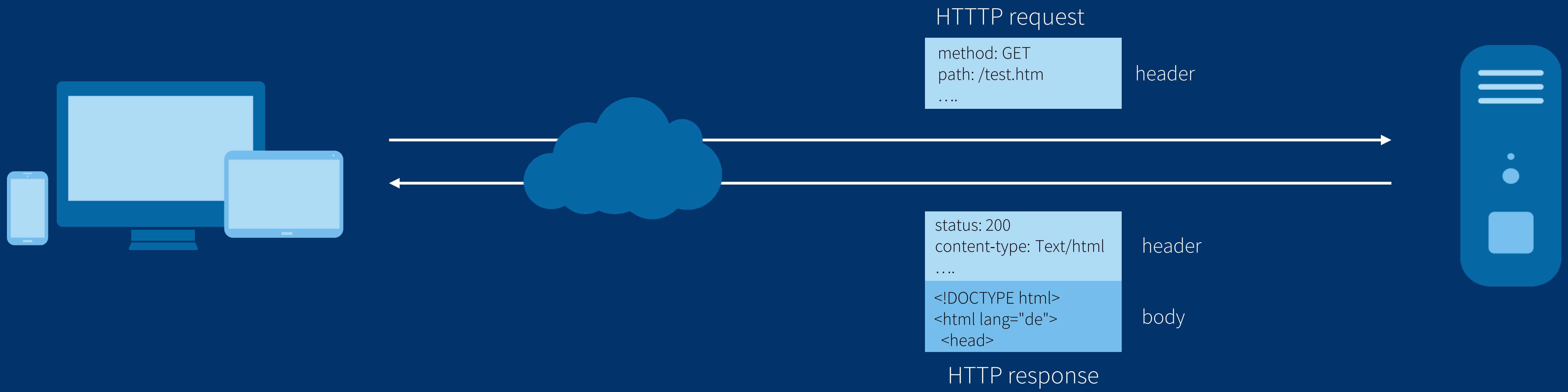
- 2009 to 2012: Software engineer in the field of web development
- Since 2012: Research assistant at the Albstadt-Sigmaringen University
  - Research project SEKT (IT Security & Smart Textiles)
  - Current & former teaching modules (selection):
    - Grundlagen der digitalen Forensik Masterstudiengang IT GRC Management
    - Digitale Forensik Bachelorstudiengang IT Security
    - Internet Grundlagen Masterstudiengang Digitale Forensik
    - Betriebssystemforensik Masterstudiengang Digitale Forensik
    - IT Security 2 Bachelorstudiengang IT Security
    - Informationssicherheit Bachelorstudiengang Wirtschaftsinformatik
    - Internettechnologien Hochschulzertifikatsprogramm
    - Cloud Technologies and Cloud Security Architectures Masterstudiengang IT GRC

Digital Forensics Investigation

- Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.
- In contradistinction to IT security, the focus of digital forensics is not on the question "What could happen?", but on "What happened?“.
- The focus of a forensic investigation is on the reconstruction of a process and the discovery or processing of anomalies such as manipulated documents (e.g. plausibility or anomalies) or deleted files (e.g. file carving).
- Digital forensic investigations usually follow the standard digital forensic process or phases which are acquisition, analysis and reporting.

HTTP Header Entries

- HTTP header fields are components of the header section of messages in the Hypertext Transfer Protocol (HTTP) [RFC4229]
- HTTP header set by both the client and the server



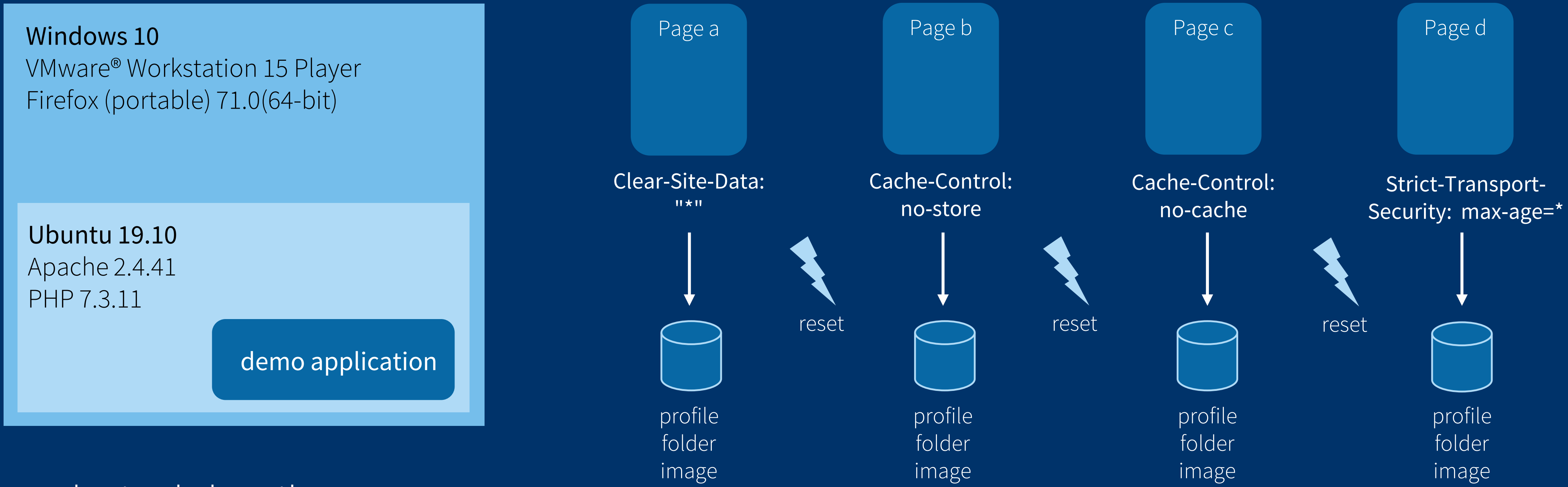
- Headers have been selected that change the behavior of the web browser when caching

Forensic Examination of Web Browser

- The forensic investigation of the web browser is of great importance, since many actions are carried out through it.
- There are certain measures to make investigations more difficult, such as “private browsing” mode or special configurations.
- However different web technologies can influence the generation of the traces. If these influences are not known, essential traces are overlooked or wrong conclusions are drawn.

- Research questions
  - *R1* Which header entry has influence on the storage of the data on the client?
  - *R2* Which header entry generates additional information outside the chronicle?

Influence on Web Browser Artifacts



Windows 10
VMware® Workstation 15 Player
Firefox (portable) 71.0(64-bit)

Ubuntu 19.10
Apache 2.4.41
PHP 7.3.11

demo application

- Technical details:
  - Host: Windows 10 (Version 1903) with VMware® Workstation 15 Player (Version 15.5.1)
  - VM: Ubuntu 19.10 with Apache (Version 2.4.41) and PHP (Version 7.3.11)
  - Firefox portable with hard drive cache and no start page

Influence on Web Browser Artifacts

Reference

- HTML, CSS, Favicon, WOFF2 Font

HTML	CSS	Image	External Font
saved	saved	saved	saved

Cache-Control [A]

- `Cache-Control: no-cache`

HTML	CSS	Image	External Font
saved	saved	saved	saved

Influence on Web Browser Artifacts

Cache-Control [B]

- `Cache-Control: no-store`

HTML	CSS	Image	External Font
not saved	saved	saved	saved

Clear-Site-Data

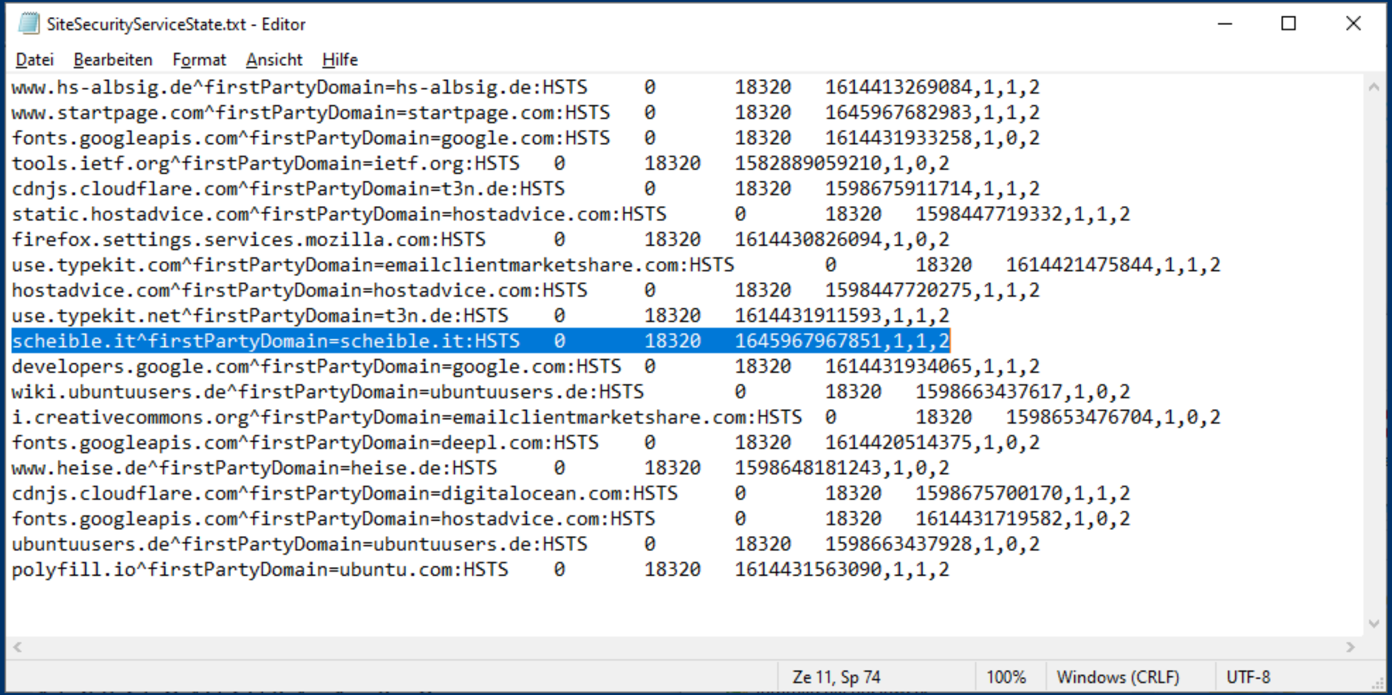
- `Clear-Site-Data: "*"`

HTML	CSS	Image	External Font
not saved	saved	saved	saved

Influence on Web Browser Artifacts

HTTP Strict-Transport-Security

- `Strict-Transport-Security: max-age=63072000`
- HSTS entries are not saved in the places.sqlite



```
www.hs-albsig.de^firstPartyDomain=hs-albsig.de:HSTS     0       18320   1614413269084,1,1,2
www.startpage.com^firstPartyDomain=startpage.com:HSTS   0       18320   1645967682983,1,1,2
fonts.googleapis.com^firstPartyDomain=google.com:HSTS   0       18320   1614431933258,1,0,2
tools.ietf.org^firstPartyDomain=ietf.org:HSTS   0       18320   1582889059210,1,0,2
cdnjs.cloudflare.com^firstPartyDomain=t3n.de:HSTS       0       18320   1598675911714,1,1,2
static.hostadvice.com^firstPartyDomain=hostadvice.com:HSTS      0       18320   1598447719332,1,1,2
firefox.settings.services.mozilla.com:HSTS      0       18320   1614430826094,1,0,2
use.typekit.com^firstPartyDomain=emailclientmarketshare.com:HSTS        0       18320   1614421475844,1,1,2
hostadvice.com^firstPartyDomain=hostadvice.com:HSTS     0       18320   1598447720275,1,1,2
use.typekit.net^firstPartyDomain=t3n.de:HSTS    0       18320   1614431911593,1,1,2
scheible.it^firstPartyDomain=scheible.it:HSTS   0       18320   1645967967851,1,1,2
developers.google.com^firstPartyDomain=google.com:HSTS  0       18320   1614431934065,1,1,2
wiki.ubuntuusers.de^firstPartyDomain=ubuntuusers.de:HSTS        0       18320   1598663437617,1,0,2
i.creativecommons.org^firstPartyDomain=emailclientmarketshare.com:HSTS  0       18320   1598653476704,1,0,2
fonts.googleapis.com^firstPartyDomain=deepl.com:HSTS    0       18320   1614420514375,1,0,2
www.heise.de^firstPartyDomain=heise.de:HSTS     0       18320   1598648181243,1,0,2
cdnjs.cloudflare.com^firstPartyDomain=digitalocean.com:HSTS     0       18320   1598675700170,1,1,2
fonts.googleapis.com^firstPartyDomain=hostadvice.com:HSTS       0       18320   1614431719582,1,0,2
ubuntuusers.de^firstPartyDomain=ubuntuusers.de:HSTS     0       18320   1598663437928,1,0,2
polyfill.io^firstPartyDomain=ubuntu.com:HSTS    0       18320   1614431563090,1,1,2
```

Conclusions and future work

Conclusions

- HTTP header entries can influence the expected traces
- New relevant traces are created by HTTP header entries

Future work

- Examine more web technologies with regard to their impact on forensic investigation
  - Comprehensive demo application
    - Can be used for teaching
    - Or for the evaluation of tools

Questions or suggestions?

Thank you very much for your attention!

- Live demonstration:
  https://lab.scheible.it/web-forensics/httpheaders/

- Presentation:
  https://scheible.it/itg-itsec_httpheaders