Household INFOSEC in a Post-Sony Era

Steve Loughran
stevel@apache.org

hadoop-trunk — fish /Users/stevel/Projects/Hortonworks/Projects/hadoop-trunk — fish — 158×43

```
[INFO] Apache Hadoop YARN Applications ..... SUCCESS [  0.037 s]
[INFO] Apache Hadoop YARN DistributedShell ..... SUCCESS [  0.576 s]
[INFO] Apache Hadoop YARN Unmanaged Am Launcher ..... SUCCESS [  0.314 s]
[INFO] Apache Hadoop YARN Site ..... SUCCESS [  0.034 s]
[INFO] Apache Hadoop YARN Registry ..... SUCCESS [  0.861 s]
[INFO] Apache Hadoop YARN Project ..... SUCCESS [  0.077 s]
[INFO] Apache Hadoop MapReduce Client ..... SUCCESS [  0.068 s]
[INFO] Apache Hadoop MapReduce Core ..... SUCCESS [  3.656 s]
[INFO] Apache Hadoop MapReduce Common ..... SUCCESS [  1.765 s]
[INFO] Apache Hadoop MapReduce Shuffle ..... SUCCESS [  0.397 s]
[INFO] Apache Hadoop MapReduce App ..... SUCCESS [  2.176 s]
[INFO] Apache Hadoop MapReduce HistoryServer ..... SUCCESS [  1.085 s]
[INFO] Apache Hadoop MapReduce JobClient ..... SUCCESS [  2.580 s]
[INFO] Apache Hadoop MapReduce HistoryServer Plugins ..... SUCCESS [  0.166 s]
[INFO] Apache Hadoop MapReduce Examples ..... SUCCESS [  1.121 s]
[INFO] Apache Hadoop MapReduce ..... SUCCESS [  0.086 s]
[INFO] Apache Hadoop MapReduce Streaming ..... SUCCESS [  0.712 s]
[INFO] Apache Hadoop Distributed Copy ..... SUCCESS [  2.001 s]
[INFO] Apache Hadoop Archives ..... SUCCESS [  0.265 s]
[INFO] Apache Hadoop Archive Logs ..... SUCCESS [  0.500 s]
[INFO] Apache Hadoop Rumen ..... SUCCESS [  0.797 s]
[INFO] Apache Hadoop Gridmix ..... SUCCESS [  0.871 s]
[INFO] Apache Hadoop Data Join ..... SUCCESS [  0.426 s]
[INFO] Apache Hadoop Ant Tasks ..... SUCCESS [  0.232 s]
[INFO] Apache Hadoop Extras ..... SUCCESS [  0.444 s]
[INFO] Apache Hadoop Pipes ..... SUCCESS [  0.075 s]
[INFO] Apache Hadoop OpenStack support ..... SUCCESS [  0.729 s]
[INFO] Apache Hadoop Amazon Web Services support ..... SUCCESS [  0.733 s]
[INFO] Apache Hadoop Azure support ..... SUCCESS [  0.692 s]
[INFO] Apache Hadoop Client ..... SUCCESS [  1.176 s]
[INFO] Apache Hadoop Mini-Cluster ..... SUCCESS [  0.223 s]
[INFO] Apache Hadoop Scheduler Load Simulator ..... SUCCESS [  1.718 s]
[INFO] Apache Hadoop Tools Dist ..... SUCCESS [  0.356 s]
[INFO] Apache Hadoop Tools ..... SUCCESS [  0.035 s]
[INFO] Apache Hadoop Distribution ..... SUCCESS [  0.079 s]
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time: 02:58 min
[INFO] Finished at: 2016-06-03T15:13:33+01:00
[INFO] Final Memory: 245M/961M
[INFO] ------------------------------------------------------------------------
~/P/H/P/hadoop-trunk (branch-2) $
```

Me: Hadoop committer; @home

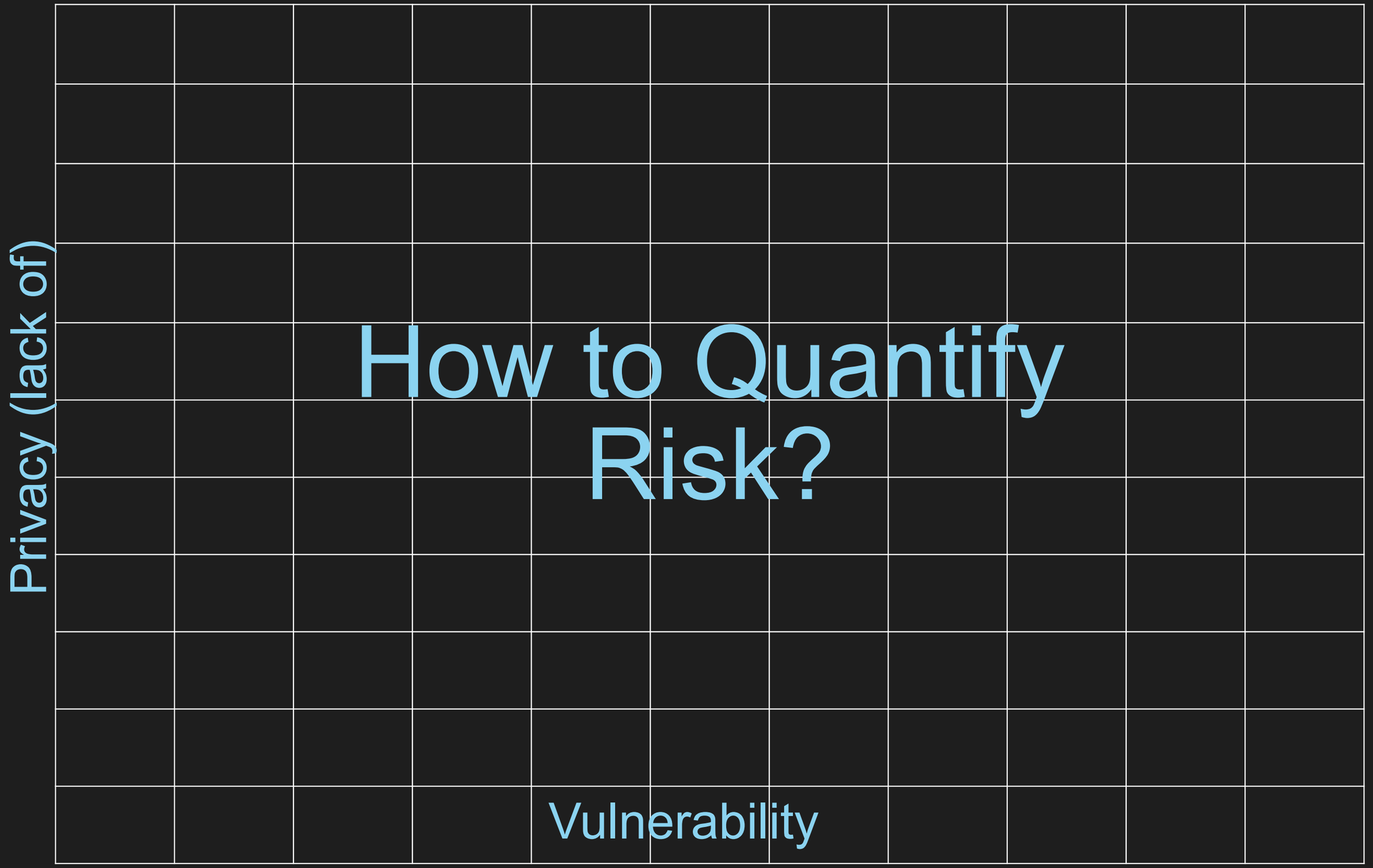

FROM THE WESTERN CAPITALIST PIGS WHO BROUGHT YOU
NEIGHBORS AND THIS IS THE END
전쟁은 시작될것이다
전쟁은 시작될것이다
SETH ROGEN JAMES FRANCO
이 무식한 미국놈들을 믿지 마십시오!
THE
인터뷰 INTERVIEW 인터뷰
전쟁은 시작될것이다
전쟁은 시작될것이다
THIS FILM IS NOT YET RATED.
FOR FUTURE INFO GO TO FILMRATINGS.COM
CHRISTMAS
/TheInterview
COLUMBIA PICTURES
★ 네이버스와 디스이즈 더 엔드를 만든 서부 자본주의 돼지들의 야심작 ★

Data Integrity
Data Privacy
Data Availability
Resource Control


UE


СССР

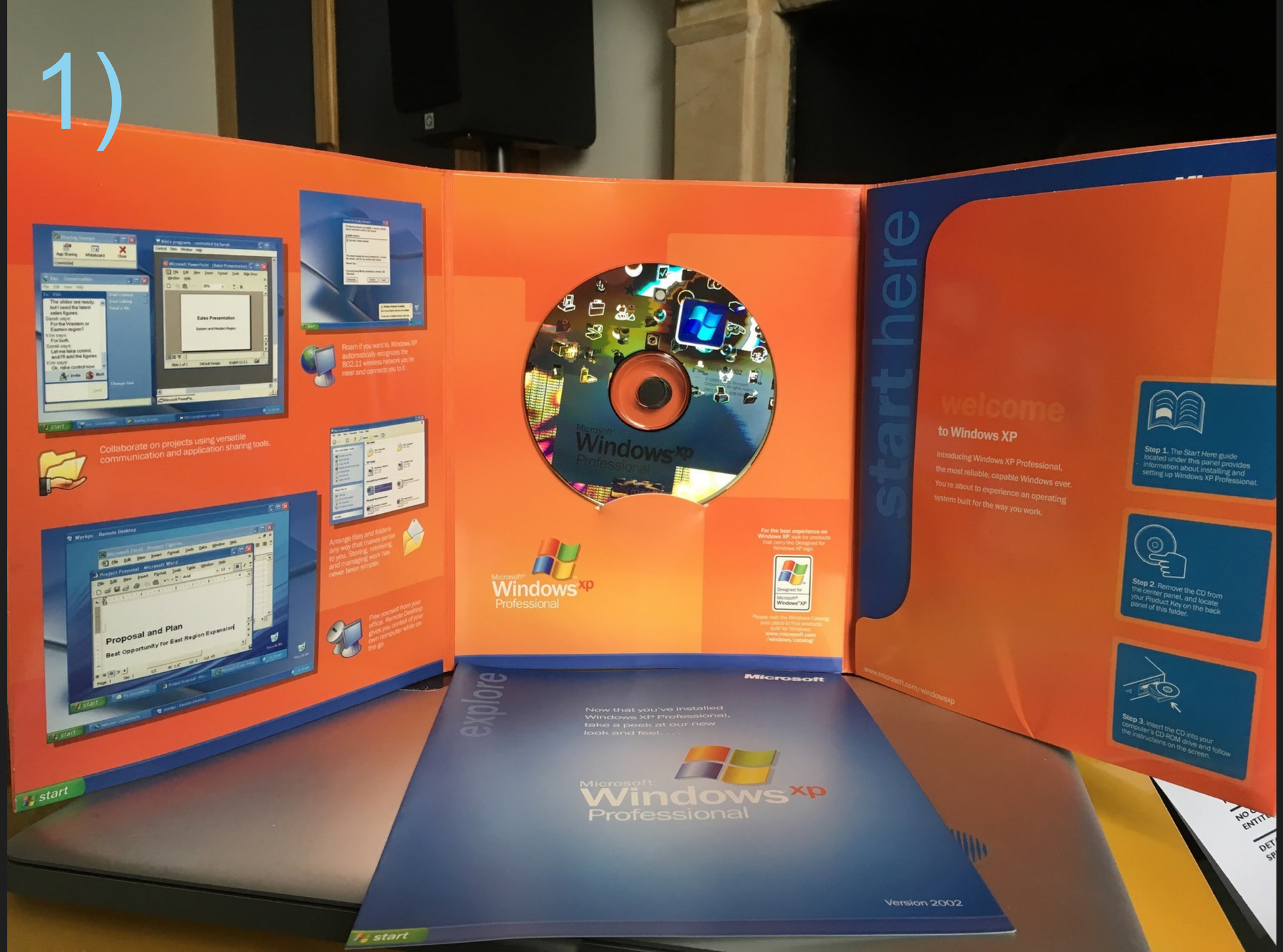

School


Privacy (lack of)
How to Quantify Risk?
Vulnerability

(1, 0)


Kerberos Diag
Kdiag:
• -h: kinit/klist
• jce
• EAR
• krb5
• native
• native mode
-- required
- "krb5"
- "yarn"
- "zookeeper"
- "dns"
auth = simple.
look a specifics
check secure dns
CAMBRIDGE

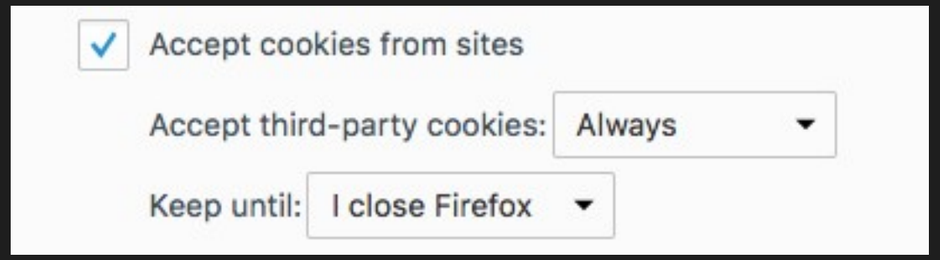
(11, 1)

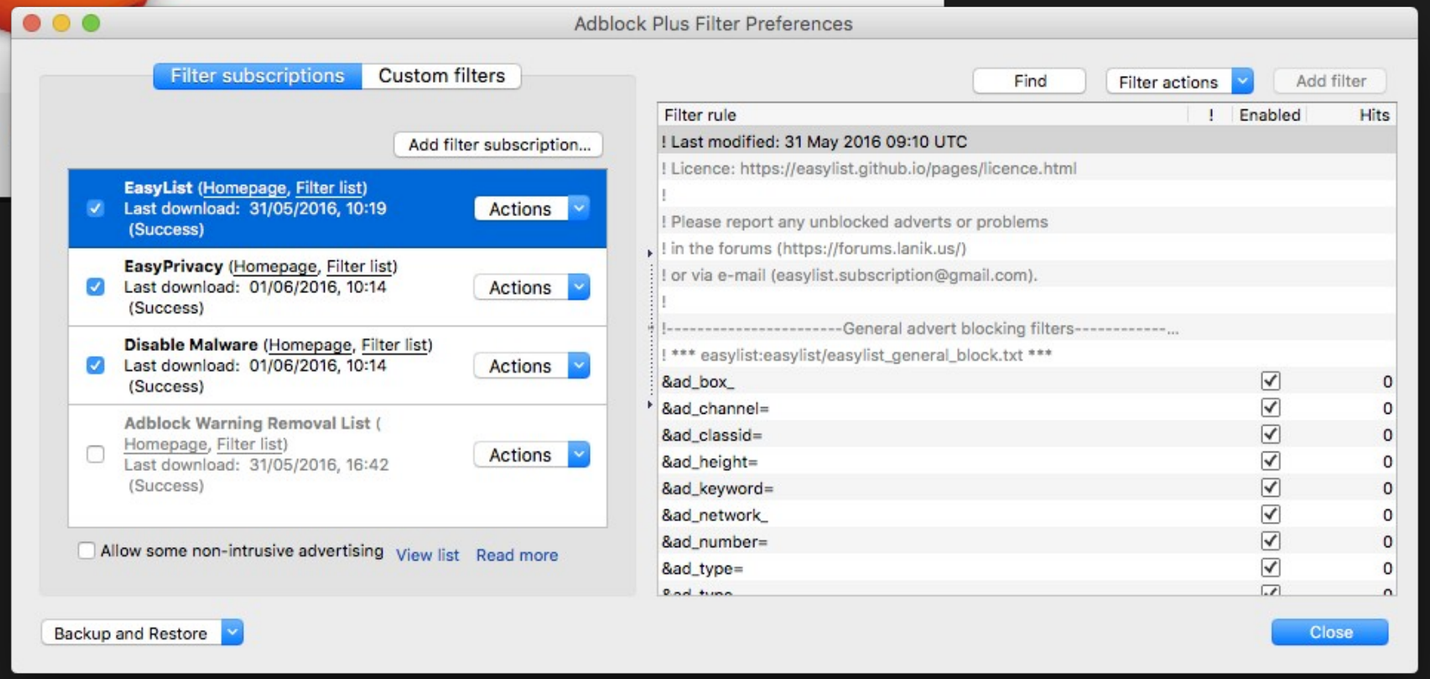

Collaborate on projects using versatile communication and application sharing tools.
Roam if you want to. Windows XP automatically recognizes the 802.11 wireless network you're near and connects you to it.
Arrange files and folders any way that makes sense to you. Storing, retrieving, and managing work has never been simpler.
Free yourself from your office. Remote Desktop gives you control of your own computer while on the go.
Proposal and Plan
Best Opportunity for East Region Expansion
Microsoft Windows xp Professional
For the best experience on Windows XP, look for products that carry the Designed for Windows XP logo.
Designed for Microsoft Windows XP
Please visit the Windows Catalog near you to find products built for Windows.
www.microsoft.com/windows/catalog/
start here
welcome
to Windows XP
Introducing Windows XP Professional, the most reliable, capable Windows ever. You're about to experience an operating system built for the way you work.
Step 1. The Start Here guide located under this panel provides information about installing and setting up Windows XP Professional.
Step 2. Remove the CD from the center panel, and locate your Product Key on the back panel of this folder.
Step 3. Insert the CD into your computer's CD-ROM drive and follow the instructions on the screen.
www.microsoft.com/windowsxp
explore
Microsoft
Now that you've installed Windows XP Professional, take a peek at our new look and feel. . . .
Microsoft Windows xp Professional
Version 2002
start

(*, 11)

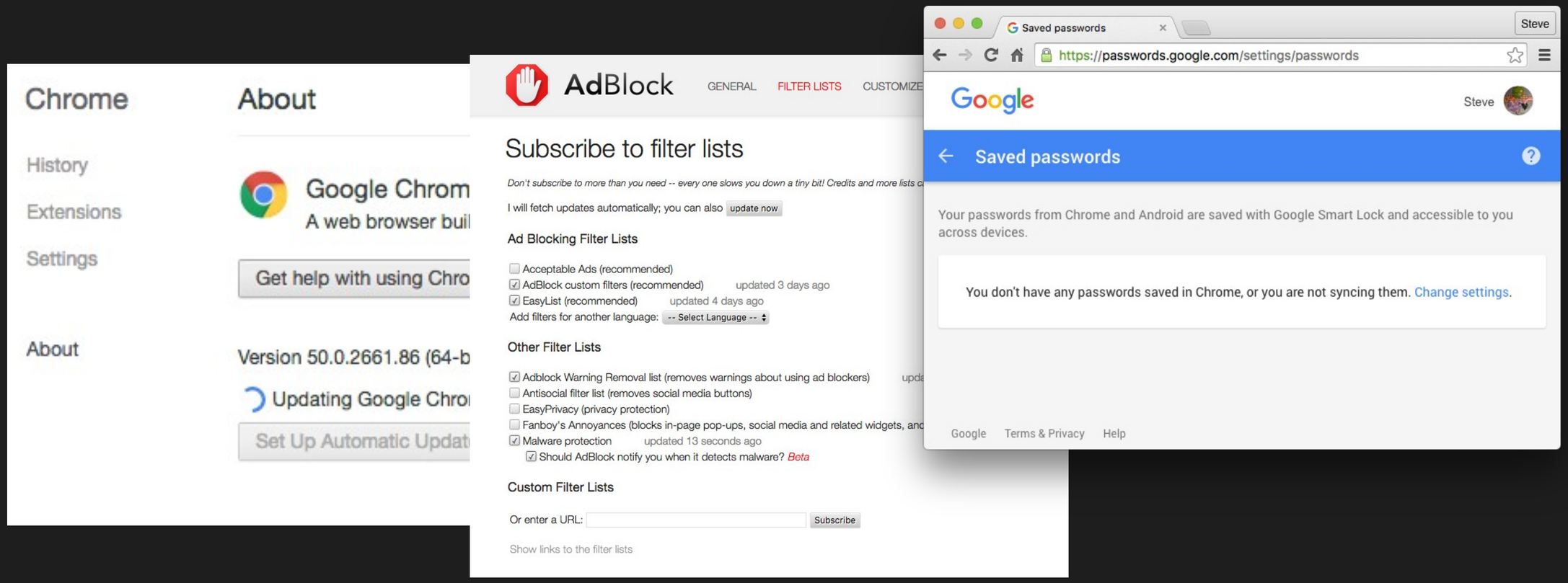
Firefox (8, 2)


Firefox
44.0.2
Downloading update — 18.1 of 31.1 MB
Firefox is designed by Mozilla, a global community working together to keep the Web open, public and accessible to all.
Want to help? Make a donation or get involved!

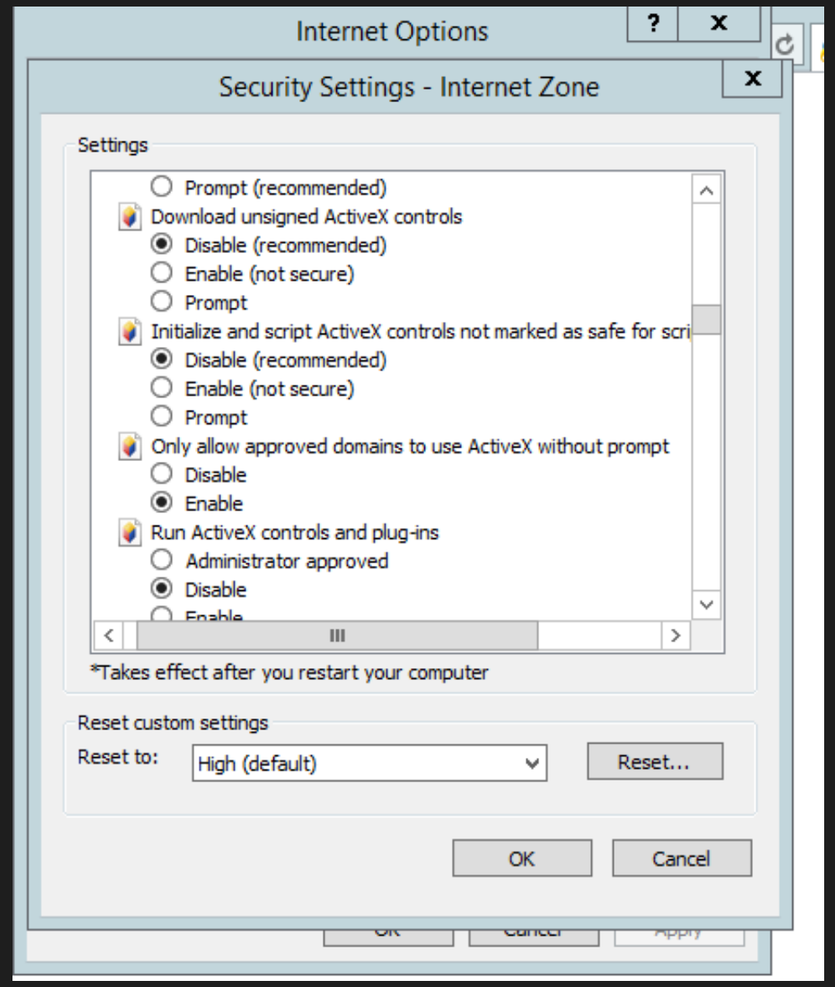

Accept cookies from sites
Accept third-party cookies: Always
Keep until: I close Firefox

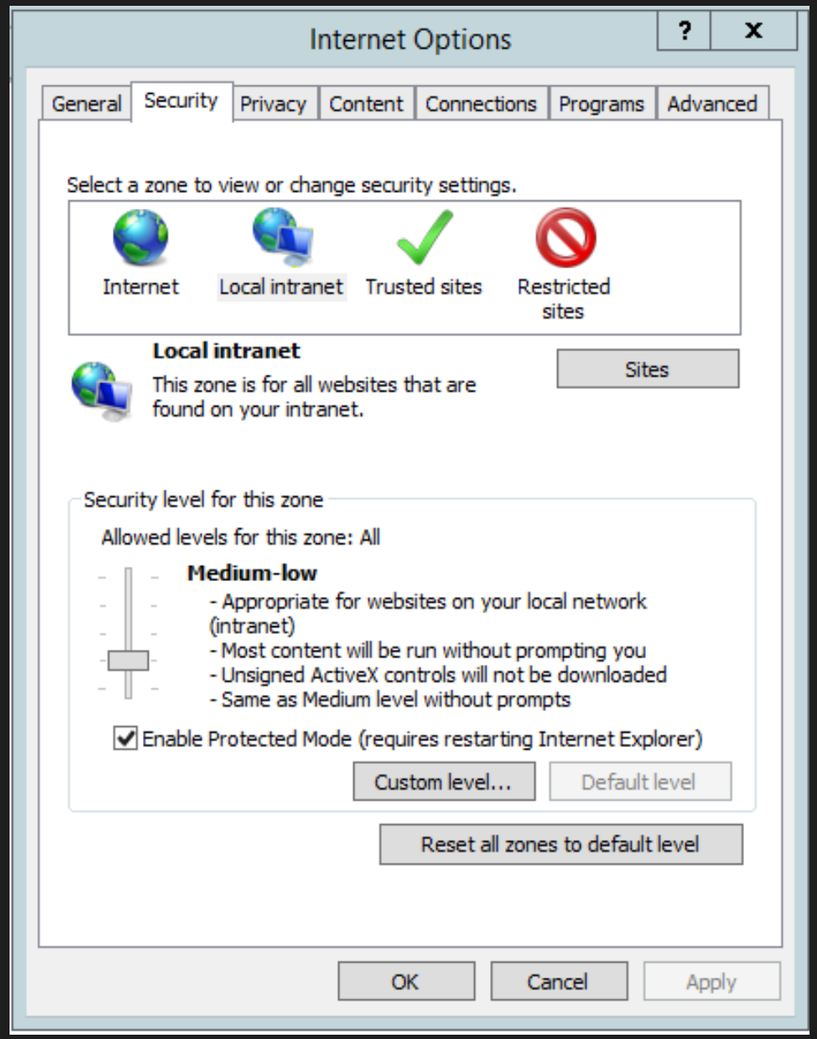

Adblock Plus Filter Preferences
Filter subscriptions
Custom filters
Add filter subscription...
EasyList (Homepage, Filter list)
Last download: 31/05/2016, 10:19
(Success)
Actions
EasyPrivacy (Homepage, Filter list)
Last download: 01/06/2016, 10:14
(Success)
Actions
Disable Malware (Homepage, Filter list)
Last download: 01/06/2016, 10:14
(Success)
Actions
Adblock Warning Removal List (Homepage, Filter list)
Last download: 31/05/2016, 16:42
(Success)
Actions
Allow some non-intrusive advertising View list Read more
Backup and Restore
Find
Filter actions
Add filter
Filter rule ! Enabled Hits
! Last modified: 31 May 2016 09:10 UTC
! Licence: https://easylist.github.io/pages/licence.html
!
! Please report any unblocked adverts or problems
! in the forums (https://forums.lanik.us/)
! or via e-mail (easylist.subscription@gmail.com).
!
!----------General advert blocking filters----------...
! *** easylist:easylist/easylist_general_block.txt ***
&ad_box_ 0
&ad_channel= 0
&ad_classid= 0
&ad_height= 0
&ad_keyword= 0
&ad_network_ 0
&ad_number= 0
&ad_type= 0
Close

Chrome: (8, 10)


Chrome
About
History
Extensions
Settings
About
Google Chrom
A web browser buil
Get help with using Chro
Version 50.0.2661.86 (64-b
Updating Google Chro
Set Up Automatic Updat
AdBlock
GENERAL
FILTER LISTS
CUSTOMIZE
Subscribe to filter lists
I will fetch updates automatically; you can also update now
Ad Blocking Filter Lists
Acceptable Ads (recommended)
AdBlock custom filters (recommended) updated 3 days ago
EasyList (recommended) updated 4 days ago
Add filters for another language: -- Select Language --
Other Filter Lists
Adblock Warning Removal list (removes warnings about using ad blockers)
Antisocial filter list (removes social media buttons)
EasyPrivacy (privacy protection)
Malware protection updated 13 seconds ago
Should AdBlock notify you when it detects malware? Beta
Custom Filter Lists
Or enter a URL:
Subscribe
Show links to the filter lists
Saved passwords
Steve
https://passwords.google.com/settings/passwords
Google
Steve
Saved passwords
Your passwords from Chrome and Android are saved with Google Smart Lock and accessible to you across devices.
You don't have any passwords saved in Chrome, or you are not syncing them. Change settings.
Google
Terms & Privacy
Help

IE: 11.
Use to D/L firefox or chrome

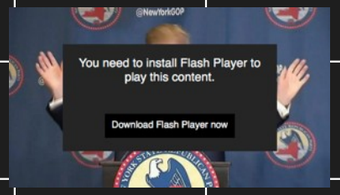




Flash (9->10, 4)

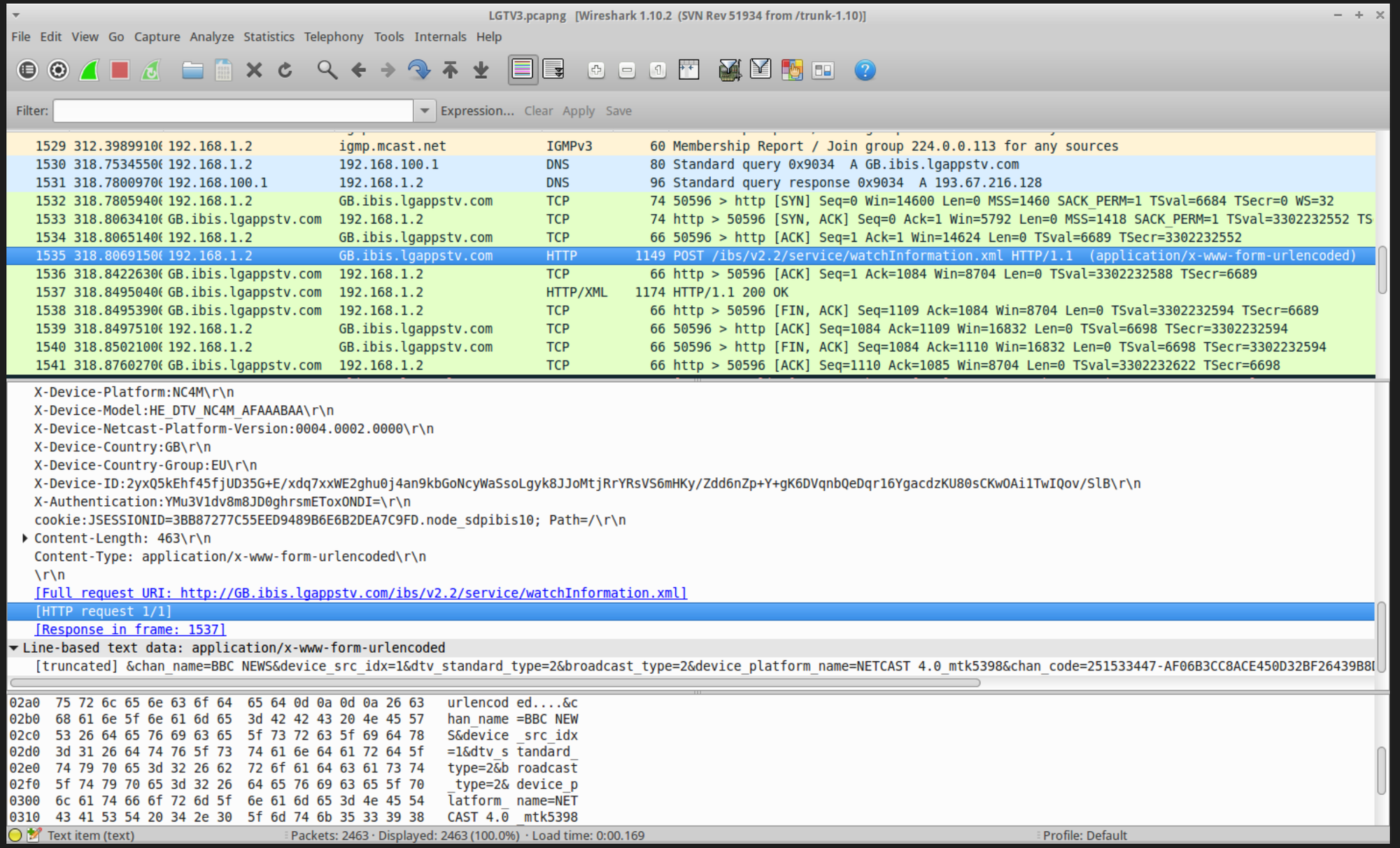

Update Adobe Flash Player
@NewYorkGOP
You need to install Flash Player to play this content.
Download Flash Player now
INSTALL

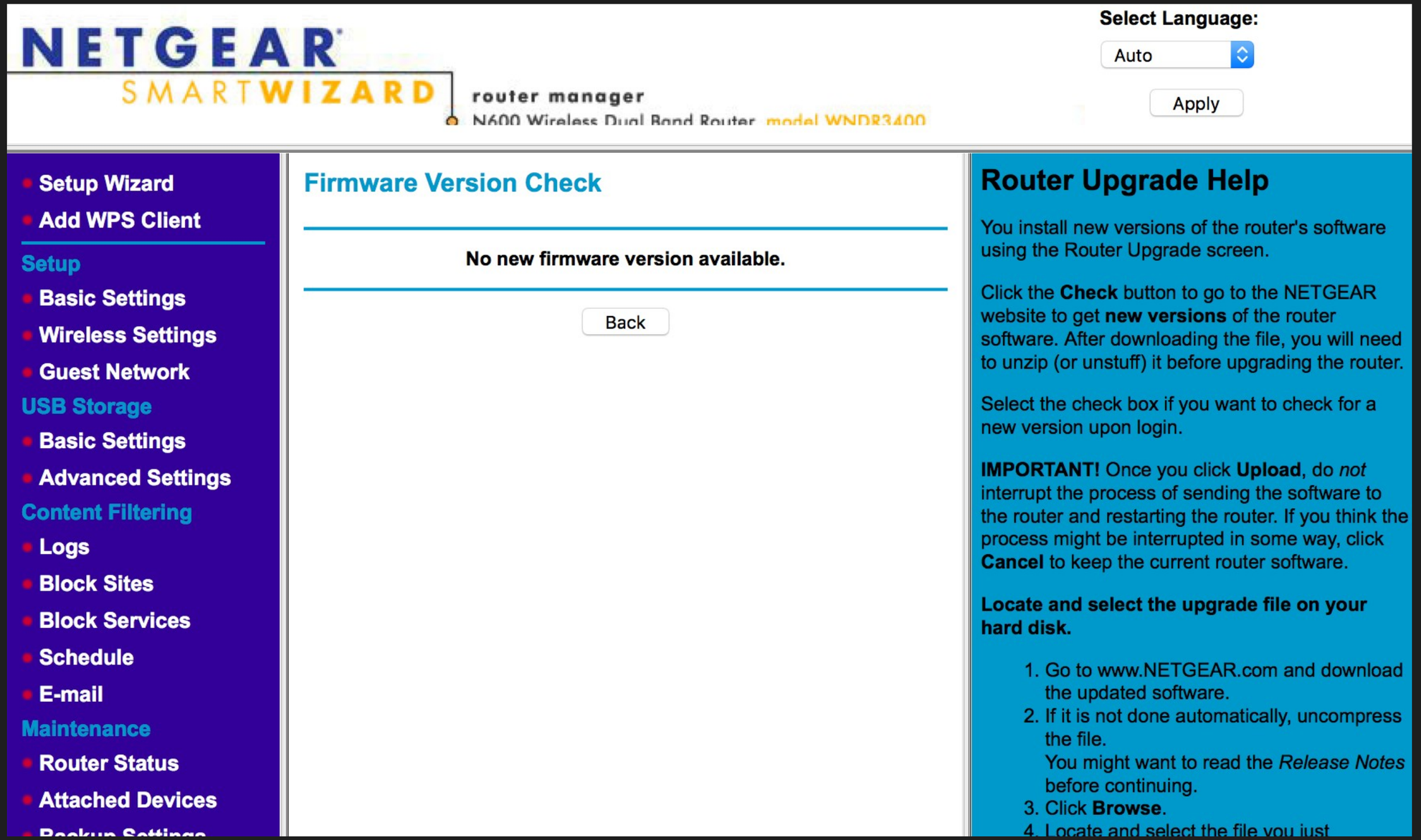
Privacy (lack of)



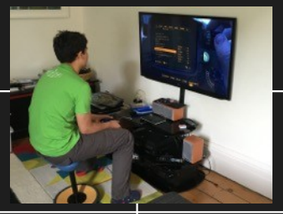
Vulnerability

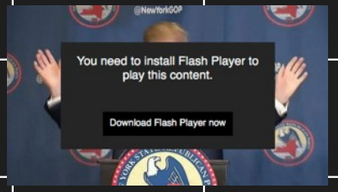

trouble—
—LG TV
iPad—
—iPhone
—PS4
-Airplay Amplifier


LGTV3.pcapng [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
1529 312.3989910(192.168.1.2 igmp.mcast.net IGMPv3 60 Membership Report / Join group 224.0.0.113 for any sources
1530 318.7534550(192.168.1.2 192.168.100.1 DNS 80 Standard query 0x9034 A GB.ibis.lgappstv.com
1531 318.7800970(192.168.100.1 192.168.1.2 DNS 96 Standard query response 0x9034 A 193.67.216.128
1532 318.7805940(192.168.1.2 GB.ibis.lgappstv.com TCP 74 50596 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=6684 TSecr=0 WS=32
1533 318.8063410(GB.ibis.lgappstv.com 192.168.1.2 TCP 74 http > 50596 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1418 SACK_PERM=1 TSval=3302232552 TS
1534 318.8065140(192.168.1.2 GB.ibis.lgappstv.com TCP 66 50596 > http [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=6689 TSecr=3302232552
1535 318.8069150(192.168.1.2 GB.ibis.lgappstv.com HTTP 1149 POST /ibs/v2.2/service/watchInformation.xml HTTP/1.1 (application/x-www-form-urlencoded)
1536 318.8422630(GB.ibis.lgappstv.com 192.168.1.2 TCP 66 http > 50596 [ACK] Seq=1 Ack=1084 Win=8704 Len=0 TSval=3302232588 TSecr=6689
1537 318.8495040(GB.ibis.lgappstv.com 192.168.1.2 HTTP/XML 1174 HTTP/1.1 200 OK
1538 318.8495390(GB.ibis.lgappstv.com 192.168.1.2 TCP 66 http > 50596 [FIN, ACK] Seq=1109 Ack=1084 Win=8704 Len=0 TSval=3302232594 TSecr=6689
1539 318.8497510(192.168.1.2 GB.ibis.lgappstv.com TCP 66 50596 > http [ACK] Seq=1084 Ack=1109 Win=16832 Len=0 TSval=6698 TSecr=3302232594
1540 318.8502100(192.168.1.2 GB.ibis.lgappstv.com TCP 66 50596 > http [FIN, ACK] Seq=1084 Ack=1110 Win=16832 Len=0 TSval=6698 TSecr=3302232594
1541 318.8760270(GB.ibis.lgappstv.com 192.168.1.2 TCP 66 http > 50596 [ACK] Seq=1110 Ack=1085 Win=8704 Len=0 TSval=3302232622 TSecr=6698
X-Device-Platform:NC4M\r\n
X-Device-Model:HE_DTV_NC4M_AFAAABAA\r\n
X-Device-Netcast-Platform-Version:0004.0002.0000\r\n
X-Device-Country:GB\r\n
X-Device-Country-Group:EU\r\n
X-Device-ID:2yxQ5kEhf45fjUD35G+E/xdq7xxWE2ghu0j4an9kbGoNcyWaSsoLgyk8JJoMtjRrYRsVS6mHKy/Zdd6nZp+Y+gK6DVqnbQeDqr16YgacdzKU80sCKwOAi1TwIQov/SlB\r\n
X-Authentication:YMu3V1dv8m8JD0ghrsmEToxONDI=\r\n
cookie:JSESSIONID=3BB87277C55EED9489B6E6B2DEA7C9FD.node_sdpibis10; Path=/\r\n
Content-Length: 463\r\n
Content-Type: application/x-www-form-urlencoded\r\n
\r\n
[Full request URI: http://GB.ibis.lgappstv.com/ibs/v2.2/service/watchInformation.xml]
[HTTP request 1/1]
[Response in frame: 1537]
Line-based text data: application/x-www-form-urlencoded
[truncated] &chan_name=BBC NEWS&device_src_idx=1&dtv_standard_type=2&broadcast_type=2&device_platform_name=NETCAST 4.0_mtk5398&chan_code=251533447-AF06B3CC8ACE450D32BF26439B8
02a0 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 0d 0a 26 63 urlencod ed....&c
02b0 68 61 6e 5f 6e 61 6d 65 3d 42 42 43 20 4e 45 57 han_name =BBC NEW
02c0 53 26 64 65 76 69 63 65 5f 73 72 63 5f 69 64 78 S&device _src_idx
02d0 3d 31 26 64 74 76 5f 73 74 61 6e 64 61 72 64 5f =1&dtv_s tandard_
02e0 74 79 70 65 3d 32 26 62 72 6f 61 64 63 61 73 74 type=2&b roadcast
02f0 5f 74 79 70 65 3d 32 26 64 65 76 69 63 65 5f 70 _type=2& device_p
0300 6c 61 74 66 6f 72 6d 5f 6e 61 6d 65 3d 4e 45 54 latform_ name=NET
0310 43 41 53 54 20 34 2e 30 5f 6d 74 6b 35 33 39 38 CAST 4.0 _mtk5398
Text item (text)
Packets: 2463 · Displayed: 2463 (100.0%) · Load time: 0:00.169
Profile: Default


NETGEAR
SMARTWIZARD
router manager
N600 Wireless Dual Band Router model WNDR3400
Select Language:
Auto
Apply
Setup Wizard
Add WPS Client
Setup
Basic Settings
Wireless Settings
Guest Network
USB Storage
Basic Settings
Advanced Settings
Content Filtering
Logs
Block Sites
Block Services
Schedule
E-mail
Maintenance
Router Status
Attached Devices
Firmware Version Check
No new firmware version available.
Back
Router Upgrade Help
You install new versions of the router's software using the Router Upgrade screen.
Click the Check button to go to the NETGEAR website to get new versions of the router software. After downloading the file, you will need to unzip (or unstuff) it before upgrading the router.
Select the check box if you want to check for a new version upon login.
IMPORTANT! Once you click Upload, do not interrupt the process of sending the software to the router and restarting the router. If you think the process might be interrupted in some way, click Cancel to keep the current router software.
Locate and select the upgrade file on your hard disk.
1. Go to www.NETGEAR.com and download the updated software.
2. If it is not done automatically, uncompress the file.
You might want to read the Release Notes before continuing.
3. Click Browse.

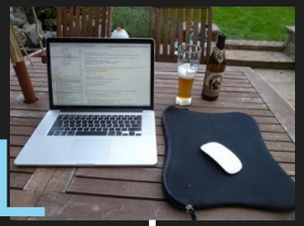
Privacy (lack of)

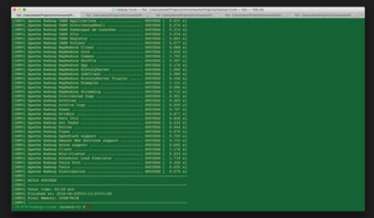


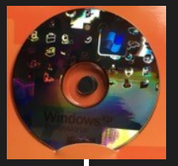


Vulnerability

CRITICAL



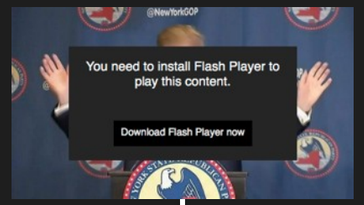




USB

DD-WRT

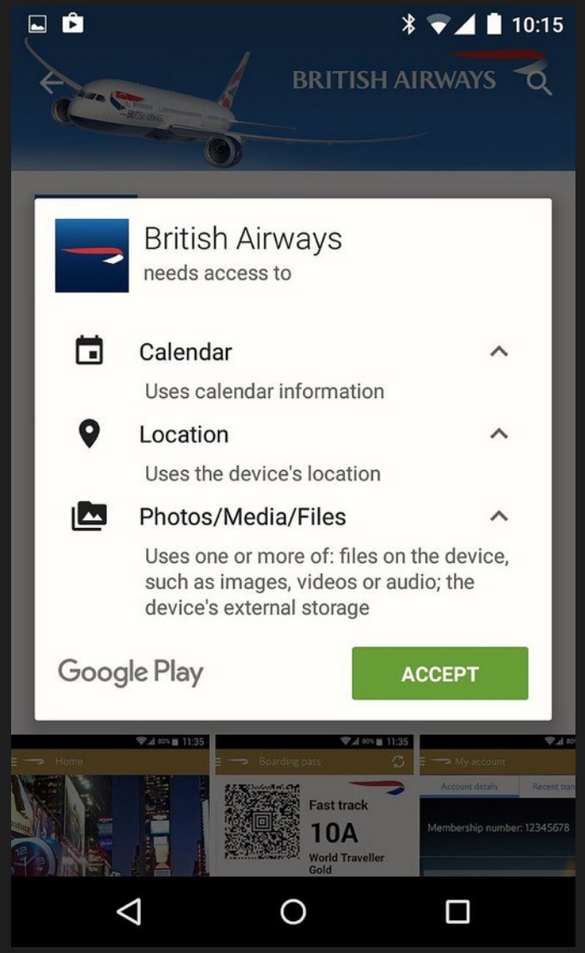
DMZ

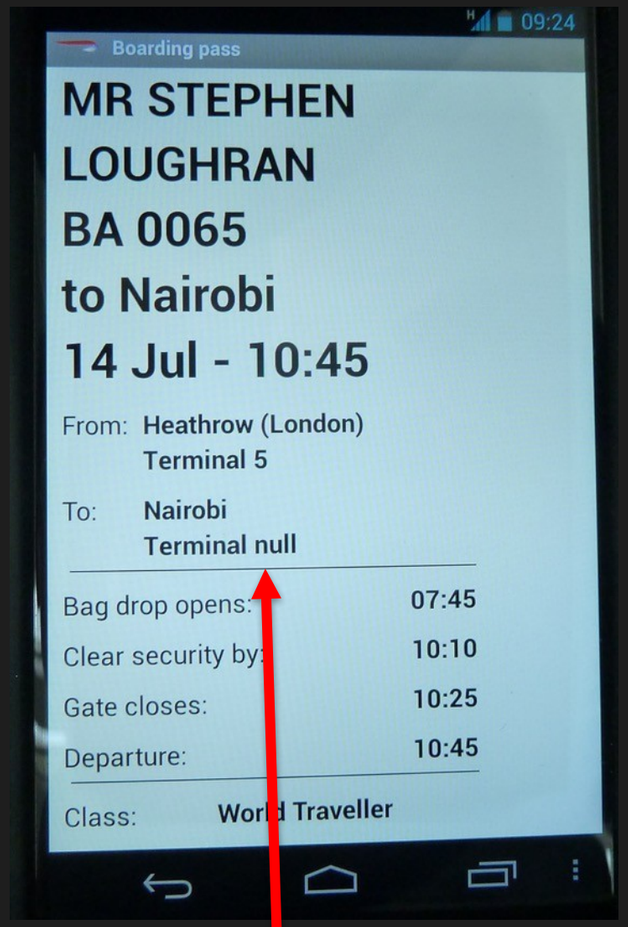


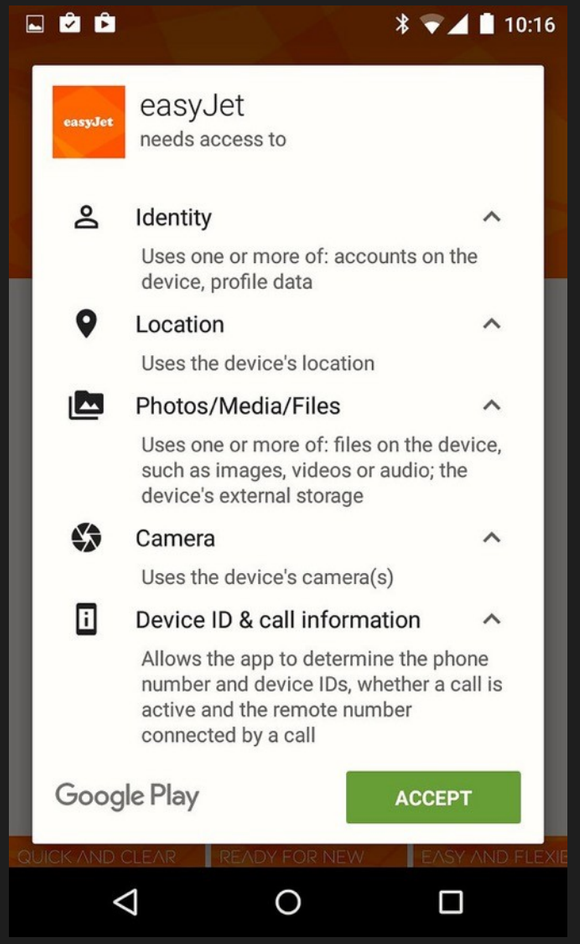
...

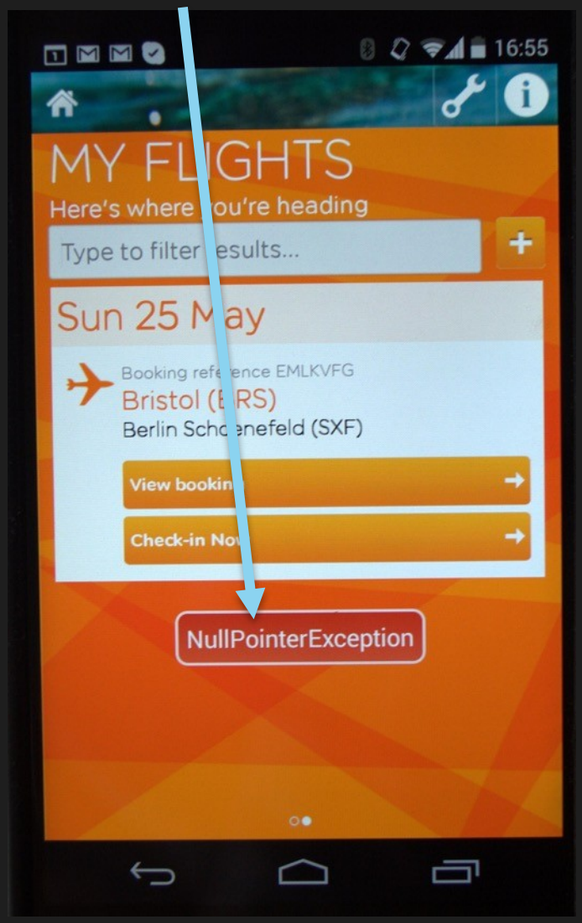
New Netgear Firewall

Other?



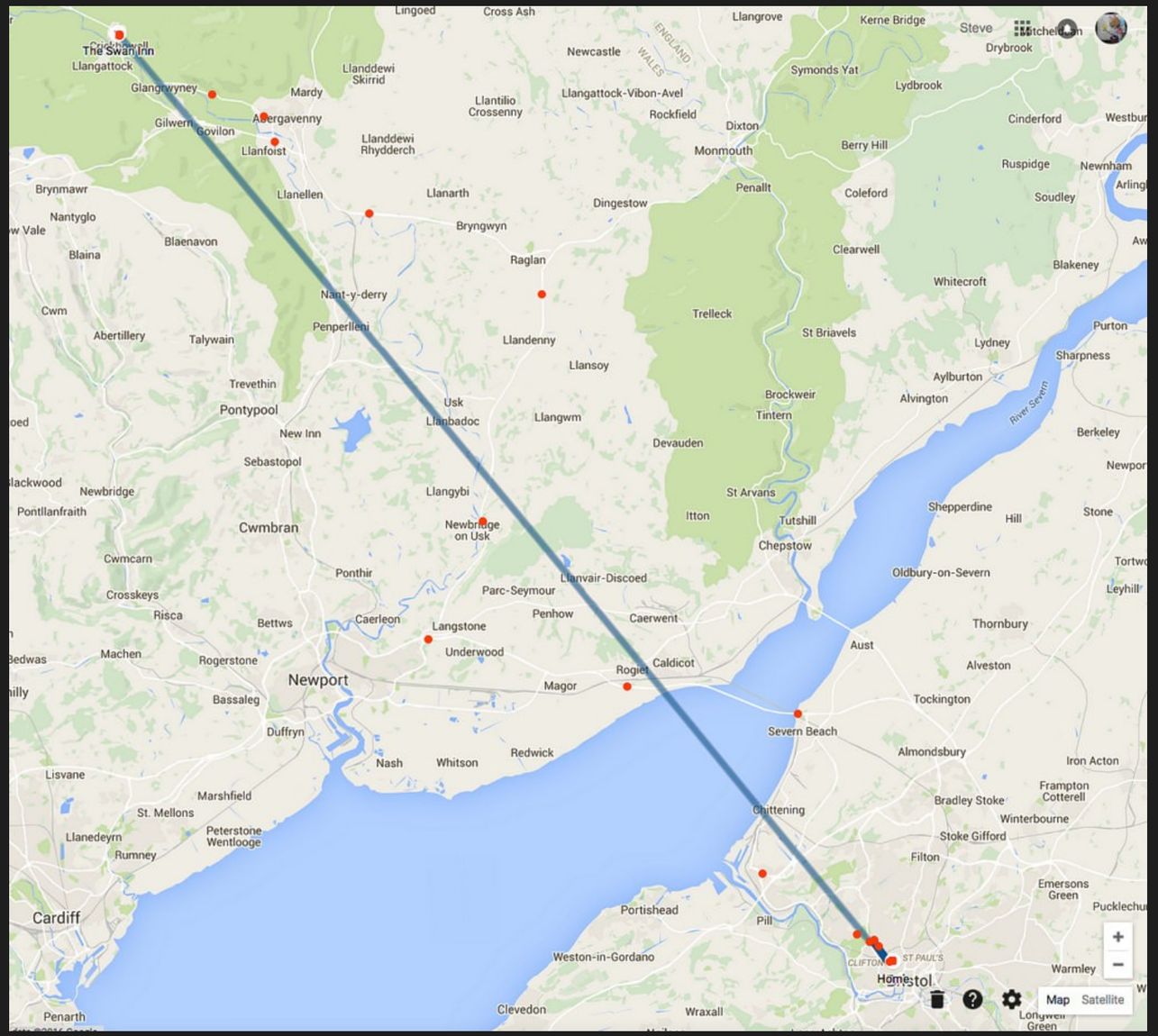


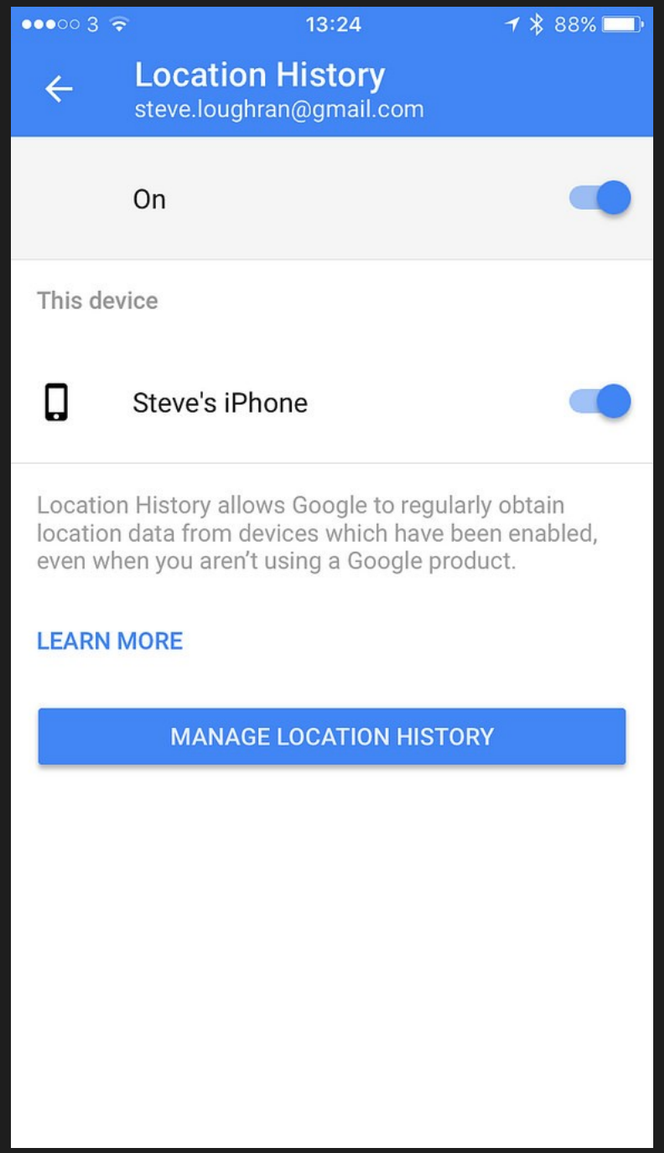




SQL validation?

(11, ?)





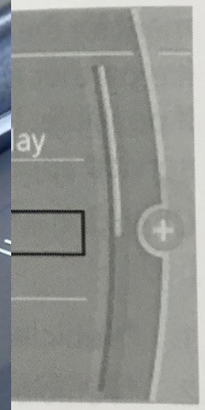
iPhone + Google photos

(5,11)


Sat 21/05
2.44 mi
summary splits
ASHLEY DOWN
REDLAND
ST WERBURGH
ST PAULS
CLIFTON
A4044
A4
Duration
26:41
Start Time
13:23
Calories Burned
296
Fats
115
Carbs
181
Average Speed
Top Speed
18.7
15:13
0.65
Speed
Heart Rate
Vale
Cotham
500ft
Home
Saint Matthews Road
Ride
15:13
Redland Rd
Fernbank Rd
Clarendon Rd
Archfield Rd
Trelawney Rd
University of Bristol
Google

(3,6+)

favourites"



ed in the his-

Settings

Activating/deactivating sound

1. Call up "Options".
2. "Sound"

Suppressing cookies

1. Call up "Options".
2. "Block cookies"

Change to mobile web page view

1. Call up "Options".
2. "Activate Flash plugin"

Suppressing pop-ups

1. Call up "Options".
2. "Block pop-ups"

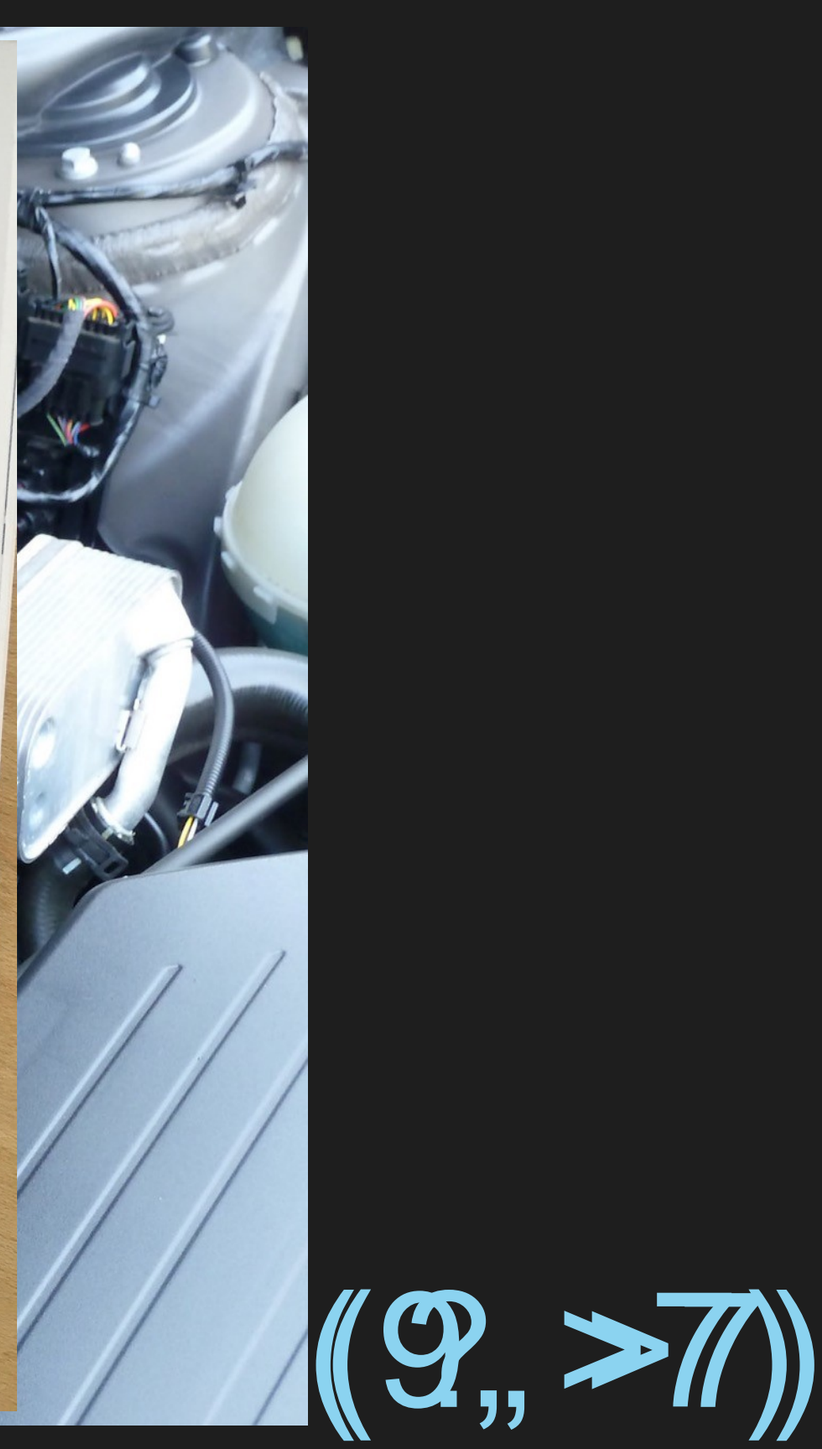
Suppress HTTPS warnings

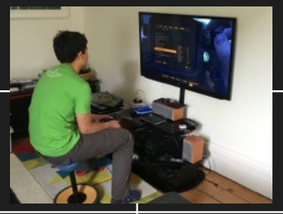
1. Call up "Options".
2. "Block warnings"

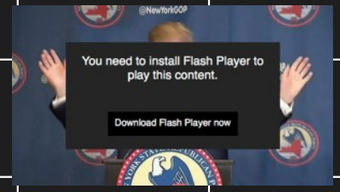
Delete personal settings

1. Call up "Options".
2. "Clear personal settings"

   HTTPS certificates and history are deleted.







Privacy (lack of)

Vulnerability


Game over
Via Reale


We must fix this in our code

All external data is malicious

All remote interactions leak privacy

```
new URL("www.starcon.net.kp").toString();
```

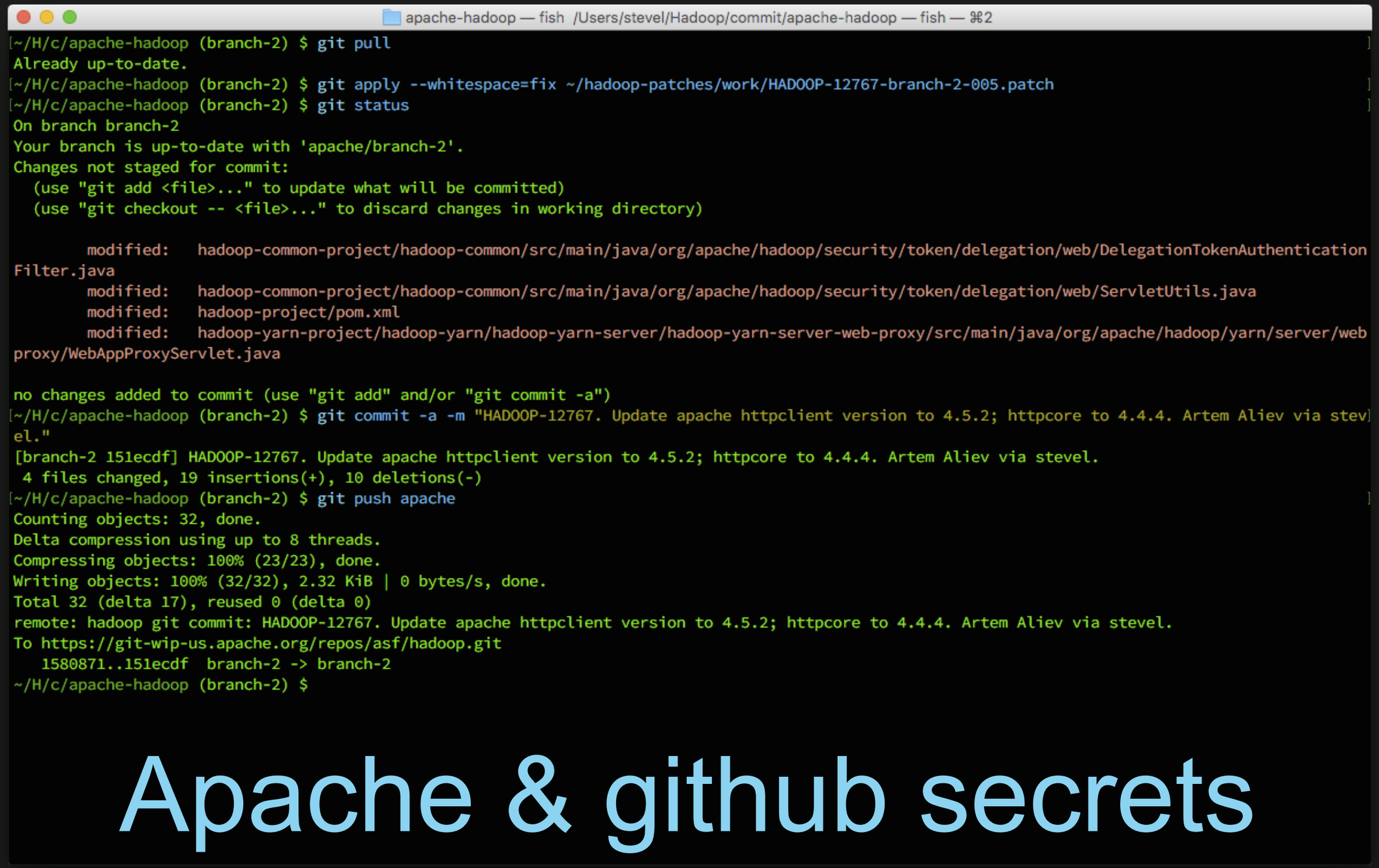
java.net.URL (>2, >2)

```
def objectFile[T: ClassTag](
  path: String,
  minPartitions: Int): RDD[T] = withScope {
  sequenceFile(path,
    classOf[NullWritable],
    classOf[BytesWritable], minPartitions)
    .flatMap(x =>
      Utils.deserialize[Array[T]](
        x._2.getBytes,
        Utils.getContextOrSparkClassLoader))
}
```

SparkContext (0, 9)

```
apt-get upgrade
brew upgrade
mvn install
npm update
yum update
pip install
docker pull
```

(?, ?)



Apache & github secrets

steve.loughran@gmail.com pwned?

Oh no — pwned!

Pwned on 1 breached site and found no pastes (subscribe to search sensitive breaches)

Notify me when I get pwned Donate

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords