



# บทที่ 3 : การป้องกันการเจาะระบบ Part2

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยต

[apipong.ping@gmail.com](mailto:apipong.ping@gmail.com)

# Agenda

▶ การควบคุมการเข้าถึง  
(Access Control)



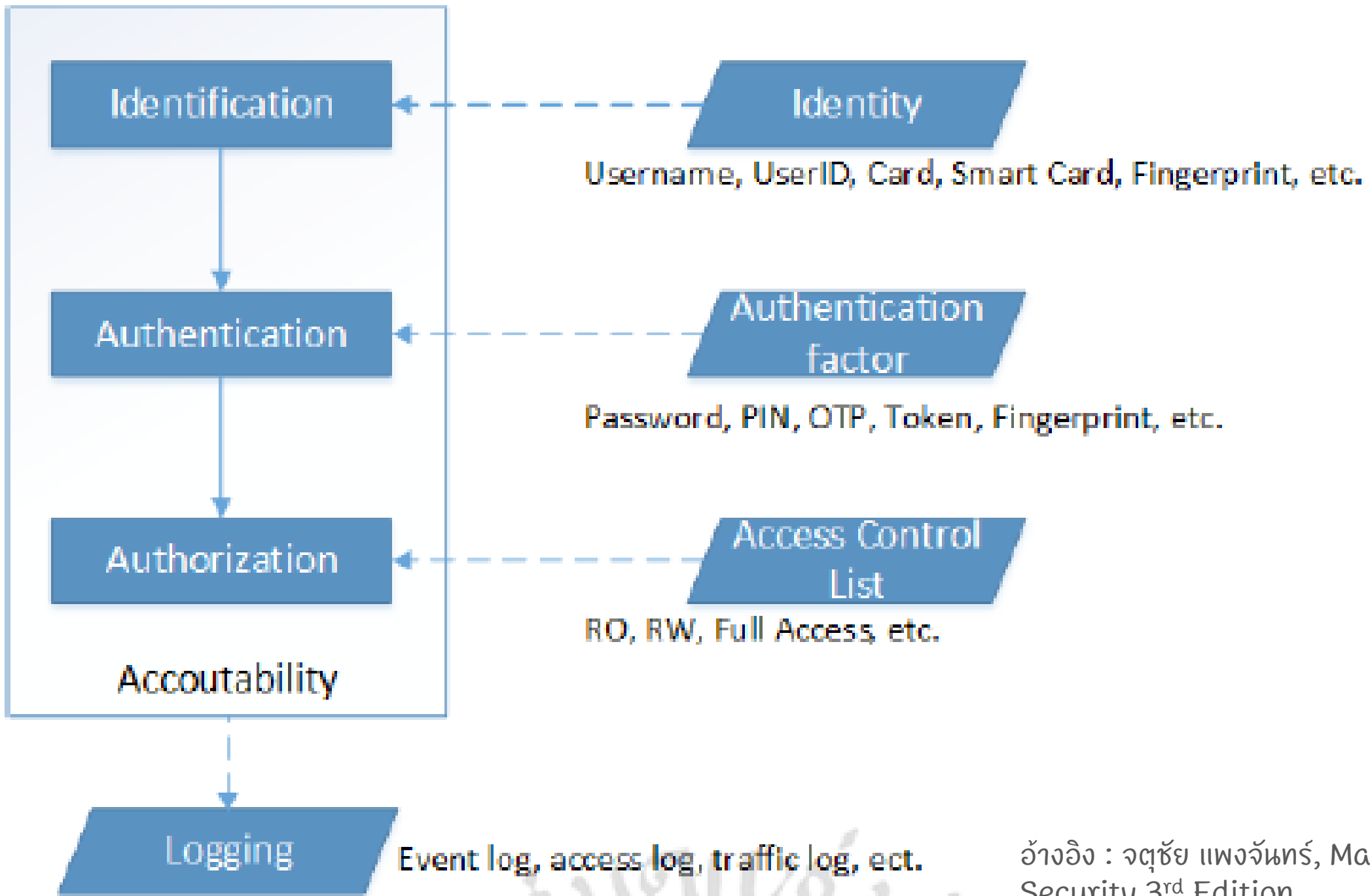
Username : admin  
Password : admin

# การควบคุมการเข้าถึง (Access Control)

มี 4 ขั้นตอนหลักๆ คือ

- การระบุตัวตน (Identification)
- การพิสูจน์ตัวตน (Authentication)
- การอนุญาต (Authorization)
- การตรวจสอบได้ (Accountability)





อ้างอิง : จตุชัย แพงจันทร์, Master in Security 3<sup>rd</sup> Edition



# การระบุตัวตน (Identification)



**การระบุตัวตน  
เป็นสิ่งที่แทน  
ตัวผู้ใช้เพื่อระบุ  
ตัวตน ปกติจะ  
ไม่ซ้ำกัน มัก  
ประกอบไปด้วย**

Username/User ID

รหัสผ่าน

ข้อมูลส่วนตัว

ชื่อหน่วยงาน

กลุ่มผู้ใช้

สิทธิ์ในการทำงาน

นโยบาย

# LDAP

(Lightweight Directory Access Protocol)

- ▶ เป็นโปรโตคอลมาตรฐานในการเข้าถึงไดเรกทอรี
- ▶ ในองค์กรจะมีไดเรกทอรีฐานข้อมูลผู้ใช้งานกลาง ซึ่งจะถูกเรียกใช้งานผ่าน LDAP

# LDAP

Lightweight Directory  
Access Protocol



## การพิสูจน์ทราบตัวตน (Authentication)

เป็นสิ่งยืนยันว่าเป็นคนนั้นหรือสิ่งนั้นจริง  
ซึ่งต้องผ่านการระบุตัวตนให้ได้ก่อน



# การพิสูจน์ทราบตัวตน 3 ประเภท

What you know



What you have



What you are



# การเดารหัสผ่าน

## (Password Guessing)

- ▶ ปกติแล้วการพิสูจน์ทราบตัวตนของผู้ใช้ จะใช้ Username และ Password โดย Username จะเป็นส่วนที่เปิดเผย แต่รหัสผ่านจะมีเฉพาะเจ้าของเท่านั้นที่ทราบ
- ▶ ผู้ใช้ส่วนใหญ่จะใช้คู่ Username และ Password สำหรับล็อกอินเข้าบัญชีในหลายๆระบบ เนื่องจากเป็นการยากที่คนอื่นๆหนึ่งจะจำรหัสผ่านได้มากมาย



Login: admin  
Password: admin



Secure enough...

## รหัสผ่านที่ถือว่ามีคุณสมบัติง่ายต่อการเดา

- ➔ รหัสผ่านที่สั้น เช่น xyz, abcd
- ➔ รหัสผ่านเดียวกับ Username
- ➔ คำที่รู้จักและคุ้นเคย เช่น password, admin
- ➔ มีข้อมูลส่วนตัวในรหัสผ่าน เช่น ชื่อ เบอร์โทร วันเกิด
- ➔ ใช้รหัสผ่านเดียวกับทุกระบบที่ใช้
- ➔ เขียนหรือจดรหัสผ่านไว้บนกระดาษแล้วเก็บไว้ในที่ที่ค้นหาได้ง่าย
- ➔ ไม่เปลี่ยนรหัสผ่านเป็นประจำ



## ระยะเวลาที่ใช้ในการเดารหัสผ่าน



Length	Lowercase	+Uppercase	+Nos. & Symbols
6 characters	10 minutes	10 hours	18 days
7 characters	4 hours	23 days	4 years
8 characters	4 days	3 years	463 years
9 characters	4 months	178 years	44,530 years











<http://randommization.com/2011/02/14/time-a-hackers-computer-takes-to-randomly-guess-your-password/>



# การป้องกันรหัสผ่าน

- ▶ อาจใช้ซอฟต์แวร์จัดการรหัสผ่าน (Password Manager) เข้ามาช่วยในการเก็บและสร้างรหัสผ่าน
- ▶ สามารถติดตั้งซอฟต์แวร์ดังกล่าวได้จากเว็บไซต์
- ▶ <http://www.pcmag.com/article2/0,2817,2407168,00.asp>

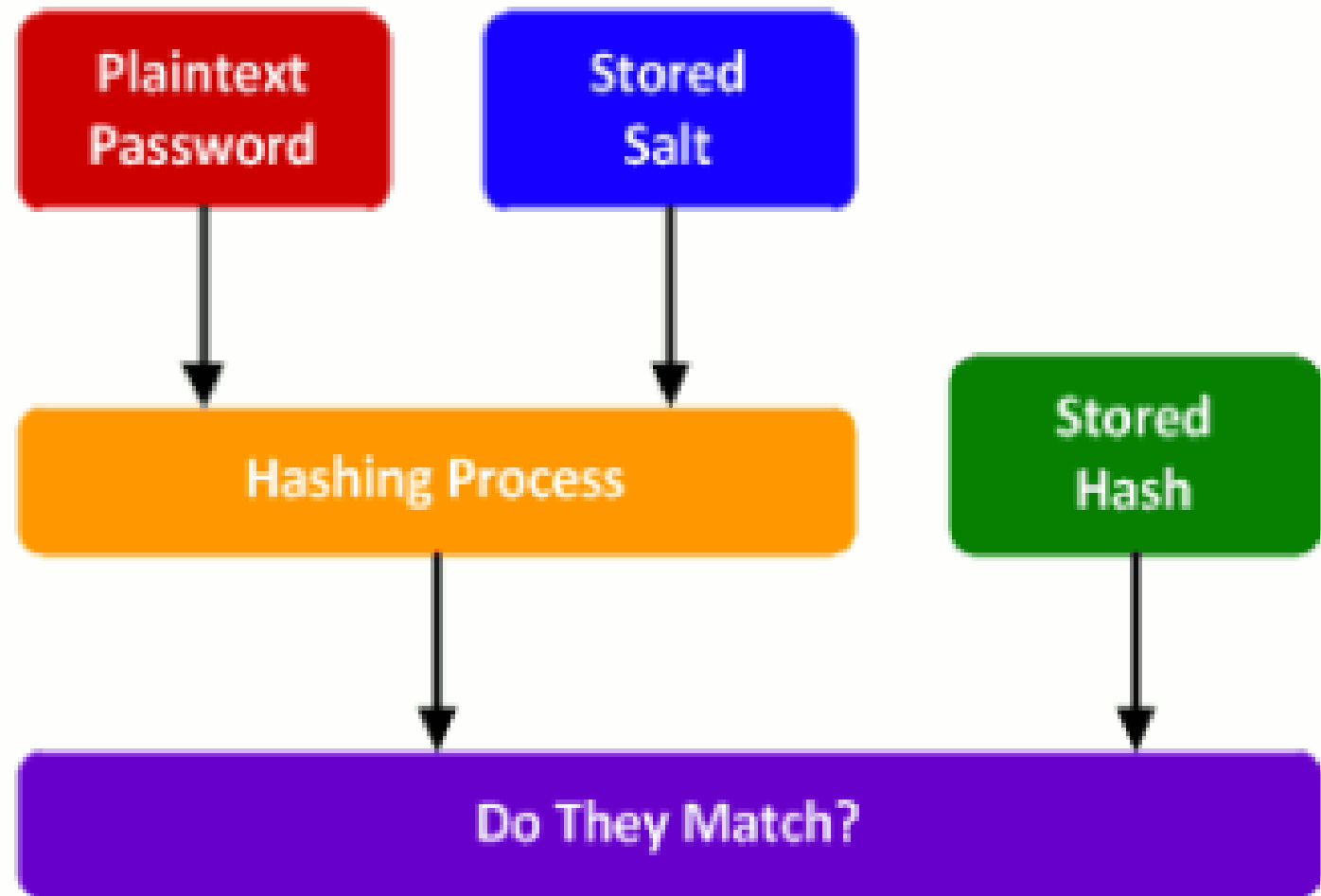
# ซอฟต์แวร์ป้องกันรหัสผ่าน

Name	Zoho Vault	Sticky Password Premium	Dashlane 4	LastPass 4.0 Premium	LogMeOnce Password Management Suite Ultimate 5.2	Keeper Password Manager & Digital Vault 10	Password Boss Premium v2.0	AgileBits 1Password 6	RoboForm 8 Everywhere	True Key by Intel Security (2017)
Lowest Price	 <b>\$12.00</b> Zoho	 <b>\$14.99</b> Special Offer	 <b>\$39.99</b> Dashlane - Synced	 <b>\$39.00</b> LogMeOnce					 <b>\$19.95</b> RoboForm	
Editors' Rating	●●●●○	●●●●● EC	●●●●● EC	●●●●● EC	●●●●● EC	●●●●○	●●●●○	●●●●○	●●●●○	●●●●○
Import From Browsers	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓
Import From Competitors	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Two-Factor Authentication	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓

## Password Creation



## Password Verification



**การเก็บรักษา Password ในฐานข้อมูลให้ปลอดภัยมากขึ้น**

Secure Password in PHP: <https://secure.php.net/manual/en/function.password-hash.php>  
And <https://secure.php.net/manual/en/function.password-verify.php>

# OTP (One-Time Password)

- เป็นรหัสผ่านที่จะมีการเปลี่ยนแปลงทุกครั้งที่มีการล็อกอินเข้าสู่ระบบ
- ออกแบบมาเพื่อป้องกันการเดารหัสผ่านและการดักฟัง
- ปกติจะใช้การส่งข้อความไปยังโทรศัพท์มือถือ (What you have) ไม่นิยมส่งทางอีเมลเพราะหากอีเมลโดนแฮ็ก จะทำให้ไม่ปลอดภัย







## Token หรือ Authenticator

- ▶ เป็นฮาร์ดแวร์หรือแอปพลิเคชันที่ใช้สร้างรหัสผ่านขณะใช้งาน และจะเปลี่ยนแปลงไปทุก ๆ ครั้ง



# Biometric

ประเภทไบโอเมตริกส์	การใช้งาน	ความแม่นยำ	การยอมรับของผู้ใช้
การลงลายเซ็น	ง่ายมาก	ต่ำ	ปานกลาง
เสียงพูด	ง่ายมาก	ต่ำ	ปานกลาง
รูปโครงหน้า	ปานกลาง	ปานกลาง	ปานกลาง
ลายฝ่ามือ	ปานกลาง	ปานกลาง	สูง
ลายนิ้วมือ	ปานกลาง	สูง	สูง
จอตาและม่านตา	ยาก	สูงมาก	ต่ำ
DNA	ยาก	สูงมาก	ต่ำ

# 2FA

## (Two-factors Authentication)

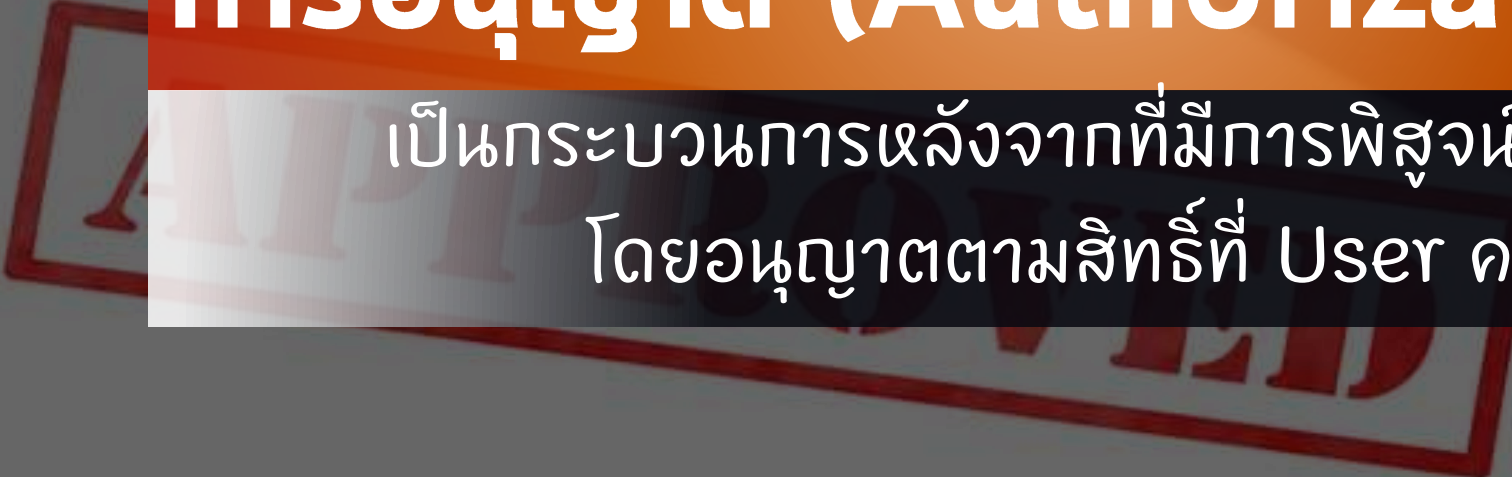
- ➔ เป็นการพิสูจน์เอกลักษณ์ฐานสองในสามหรือมากกว่า ได้แก่ สิ่งที่คุณรู้ สิ่งที่คุณมี และสิ่งที่เป็น
- ➔ เช่น ใช้รหัสผ่านคู่กับลายนิ้วมือ หรือรหัสผ่านคู่กับโทเคน





# การอนุญาต (Authorization)

เป็นกระบวนการหลังจากที่มีการพิสูจน์ตัวตนแล้ว  
โดยอนุญาตตามสิทธิ์ที่ User คนนั้นหรือสิ่งนั้นมี





## การอนุญาตแบ่งเป็น 3 ทาง

- ▶ อนุญาตเป็นรายๆ (ไม่นิยมใช้)
- ▶ อนุญาตเป็นกลุ่ม (นิยมใช้ทั่วไป)
- ▶ อนุญาตเข้าใช้หลาย ๆ ระบบ (Single Sign-on)  
นิยมใช้ในองค์กรที่มีระบบมากๆ



## การตรวจสอบได้ (Accountability)

เป็นขั้นตอนเพื่อตรวจสอบย้อนกลับเหตุการณ์ที่เกิดขึ้นในระบบ

# การเก็บล็อก (Log)

- ล็อกเป็นการเก็บเหตุการณ์ต่าง ๆ ที่เกิดขึ้นภายในระบบ
- เป็นสิ่งสำคัญมากในการสืบสวนการโจมตี
- ใช้เป็นหลักฐานทางกฎหมายได้
- แฮกเกอร์มักทำการลบล็อกเมื่อเข้าโจมตีระบบแล้ว
- ควรมีระบบจัดเก็บล็อกที่ปลอดภัย เช่น ใน Linux จะมีเซิร์ฟเวอร์สำหรับเก็บ Syslog โดยเฉพาะ

IP Address	Date	Request	Status	Size	Country	Referer
199.30.24.152	4/4/2015 2:19:12 PM	GET /images/iannetlogo3.gif HTTP/1.1	200	95405	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /images/PostHeadericon.png HTTP/1.1	200	147	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /images/nav.png HTTP/1.1	200	626	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /s_linkedicon.png HTTP/1.1	200	4029	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /images/PostQuote.png HTTP/1.1	200	445	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /s_twittericon.png HTTP/1.1	200	4992	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /images/Block-s.png HTTP/1.1	200	639	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /images/Block-h.png HTTP/1.1	200	3063	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:13 PM	GET /images/Block-v.png HTTP/1.1	200	4648	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:14 PM	GET /images/Block-c.png HTTP/1.1	200	308	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:14 PM	GET /images/BlockHeadericon.png HTTP/1.1	200	313	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:14 PM	GET /images/Footer.png HTTP/1.1	200	1352	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:14 PM	GET /images/item-separator.png HTTP/1.1	200	139	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:14 PM	GET /iannet_logo.swf HTTP/1.1	200	1658	United States	http://iannet.org/iannet_logo.swf
157.55.39.71	4/4/2015 2:19:15 PM	GET /robots.txt HTTP/1.1	200	422	United States	-
202.46.54.43	4/4/2015 2:19:38 PM	HEAD /apps/SiteVerify/ HTTP/1.1	200	0	China	-
202.46.49.12	4/4/2015 2:19:39 PM	GET /apps/SiteVerify/ HTTP/1.1	200	4302	China	-
202.46.62.24	4/4/2015 2:19:40 PM	HEAD /apps/download.php?new=1 HTTP/1.1	404	0	China	http://www.iannet.org/apps/SiteVerif
202.46.53.68	4/4/2015 2:19:41 PM	GET /apps/download.php?new=1 HTTP/1.1	404	215	China	http://www.iannet.org/apps/SiteVerif
202.46.52.25	4/4/2015 2:19:42 PM	HEAD /apps/SiteVerify/download.php?new=1 HTTP/1.1	302	0	China	http://www.iannet.org/apps/SiteVerif
202.46.52.25	4/4/2015 2:19:42 PM	HEAD /apps/SiteVerify/siteverify.zip HTTP/1.1	200	0	China	http://www.iannet.org/apps/SiteVerif
191.236.33.18	4/4/2015 2:19:50 PM	GET / HTTP/1.1	200	15947	United States	-
36.76.244.171	4/4/2015 2:20:13 PM	GET /apps/TunnelBrokerUpdate/currentver.php?v=1,14 HTTP/1.1	200	4	Indonesia	-
180.76.5.72	4/4/2015 2:20:28 PM	GET /apps/GenerateHtPassWd HTTP/1.1	301	253	China	-
180.76.5.148	4/4/2015 2:20:29 PM	GET /apps/GenerateHtPassWd/ HTTP/1.1	200	2646	China	-
202.46.63.129	4/4/2015 2:20:54 PM	HEAD /apps/TunnelBrokerUpdate/download.php HTTP/1.1	200	0	China	-
202.46.57.69	4/4/2015 2:20:56 PM	GET /apps/TunnelBrokerUpdate/download.php HTTP/1.1	200	3832	China	-
202.46.62.33	4/4/2015 2:20:56 PM	GET /apps/TunnelBrokerUpdate/download.php HTTP/1.1	200	3832	China	-
202.46.54.39	4/4/2015 2:20:57 PM	HEAD /apps/TunnelBrokerUpdate/TunnelBrokerUpdate.zip HTTP/1.1	200	0	China	http://www.iannet.org/apps/TunnelB
202.46.53.33	4/4/2015 2:20:58 PM	HEAD /apps/TunnelBrokerUpdate/download.php?new=1 HTTP/1.1	200	0	China	http://www.iannet.org/apps/TunnelB
202.46.57.83	4/4/2015 2:20:59 PM	GET /apps/TunnelBrokerUpdate/download.php?new=1 HTTP/1.1	200	3832	China	http://www.iannet.org/apps/TunnelB
202.46.54.40	4/4/2015 2:21:00 PM	HEAD /apps/TunnelBrokerUpdate/download.php/download.php?new=...	200	0	China	http://www.iannet.org/apps/TunnelB
202.46.55.28	4/4/2015 2:21:01 PM	GET /apps/TunnelBrokerUpdate/download.php/download.php?new=1 ...	200	3832	China	http://www.iannet.org/apps/TunnelB
202.46.48.26	4/4/2015 2:21:01 PM	HEAD /download.php?new=1 HTTP/1.1	404	0	China	http://www.iannet.org/apps/TunnelB
202.46.57.82	4/4/2015 2:21:02 PM	GET /download.php?new=1 HTTP/1.1	404	215	China	http://www.iannet.org/apps/TunnelB

# Apache Log Viewer