CERIAS

The Center for Education and Research in Information Assurance and Security

WHATSAPP FORENSICS: LOCATING ARTIFACTS ON WEB CLIENTS AND STANDALONE DESKTOP APPLICATIONS

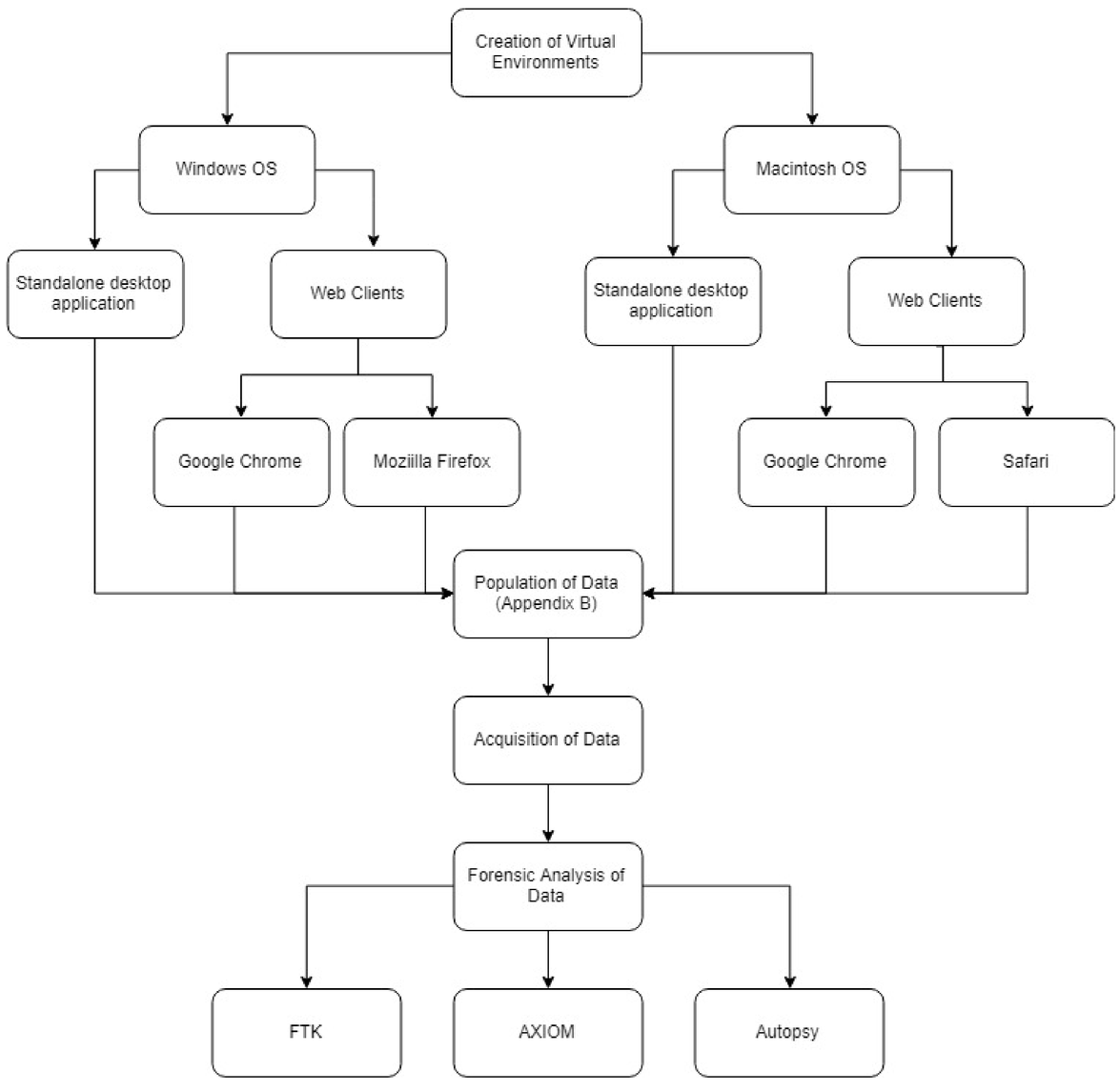
Nicolás Villacís Vukadinović, Dr. Kathryn Seigfried-Spellar, Dr. Marcus Rogers & Dr. Umit Karabiyik
Computer and Information Technology
Cyber Forensics Laboratory

WhatsApp

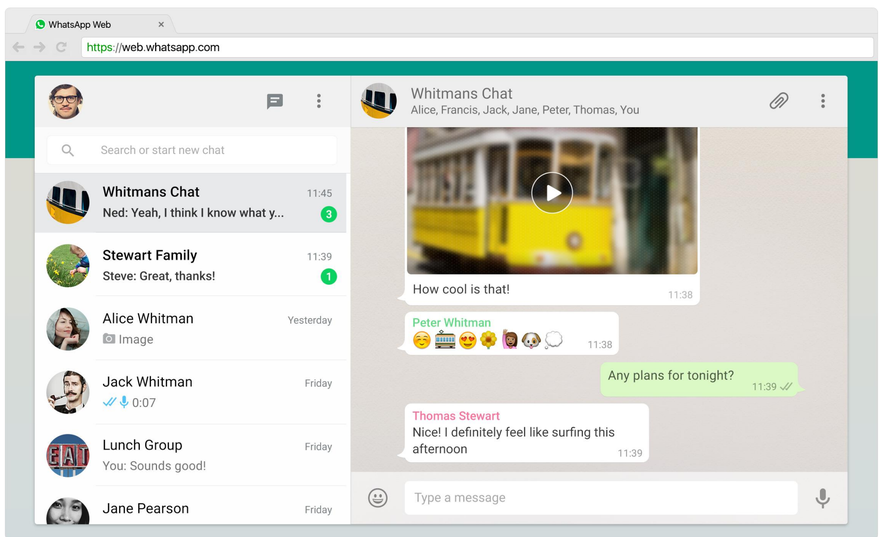
Facts

- Most popular instant messaging application worldwide
- 1.5 billion monthly active users (July 2018)
- Used in over 180 countries

Study flowchart



WhatsApp web client user interface



WhatsApp log file artifacts

Category	Artifact
Timestamps/ actions	action,presence,[available/unavailable]
	action,chatstate,[composing/paused/recording]
	action,message,[image/video/chat/vcard/document/ptt]
	action,msgs,delete
	action,block,true,18125730324
	action,battery,84,false
	action,group,create
	action,set_pic,17653278892@c
	action,pushname
	action,status,set
	action,chat,read,{"fromMe":false,"remote":18125730324@c.us…}
	action,status,read,{"fromMe":false,"remote":"s&ð>@broadcast","id":"C259586486C33C79E0482B1F346C9D98…}"
	Media:sendToChat chat 18125730324@c.us
	Media:sendToChat chat 17653278892-1548963594@g.us
	action,msg,relay,[chat,image,video],18125730324@c.us,17653278892@c.us
	action,msg,relay,image,status@broadcast,17653278892@c.us,false_status@broadcast_FCECD863D949D0AAD2DFE7260AD9DC4B,18125730324@c.us"
	profilePic:cache-save: profile_pic_thumb
	AppUpdate:update current: 0.3.2041 latest: 0.3.2041
Mobile device information	webcPhoneOsBuildNumber = PQ1A.181205.002.A1
	webcPhoneOsVersion = 9
	webcPhoneAppVersion = 2.19.17
	webcPhoneDeviceManufacturer = Google
	webcPhoneDeviceModel = marlin
	webcPhoneCharging = false
Browser user agent	userAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.81 Safari/537.36

Note. All timestamps/actions begin with a date and time (i.e., YYYY-MM-DD HH:MM:SS.MS).

Findings:

- WhatsApp log file, main source of artifacts
- Cached profile pictures
- Application run count/time/date
- URL visit count/time/date
- Overall, Chrome/Firefox web clients log the most information

PURDUE UNIVERSITY Discovery Park

PURDUE UNIVERSITY Cyber Forensics

CERIAS