

The background of the slide features a person wearing a grey hoodie, seen from behind, sitting at a desk. A computer monitor is visible in front of them, displaying some code. The entire scene is overlaid with a dense pattern of green and blue binary digits (0s and 1s), creating a digital or cyber-themed atmosphere.

INCS-712: Digital Forensics

Chapter 4 - Digital Forensic Tools

Baljeet Malhotra, PhD

Recall - Basic Methodology



Acquire the evidence (without altering/damaging)



Authenticate the evidence (of crime scene)



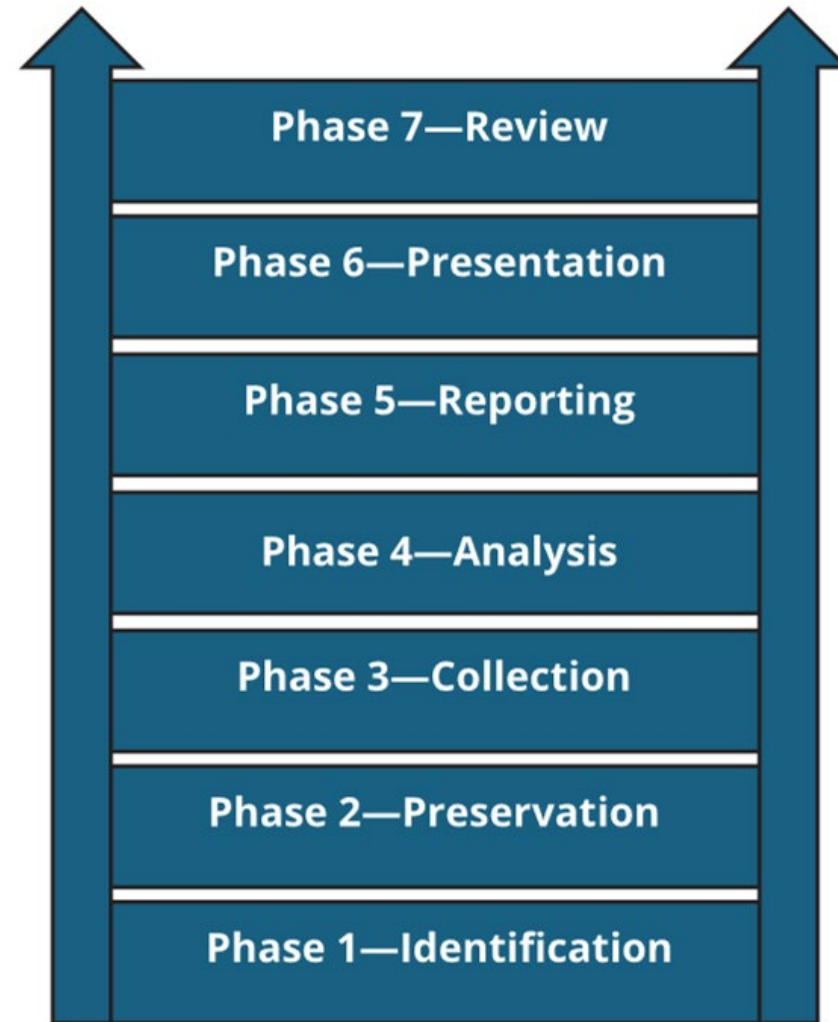
Analyze the data (without modifying it)



Apply the analytics to substantiate

Recall - Digital Forensic Process

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Reporting
- Presentation



Digital Forensic Workflow and Tools



ACQUIRE

Image Creation,
Authentication,
Mounting



DISCOVER

Data, Metadata,
Accurate Bill of
Materials (BoMs)



IDENTIFY

Security, Legal
Technical, and
Compliance Items



VALIDATE

Scenarios and
Hypothesis
Periodically



ALERT

Stakeholders for
Business-Critical
Impact



RECOMMEND

Actions, Policies,
Compensation to
Affected Parties

- Imaging and Mounting
- Memory Analysis
- Registry Analysis
- Packet Analysis
- Hash Analysis

- Metadata/Secondary Data
- Compliance/Statutory Data
- Laws and Regulations
- Reports and Memos
- Communications



INCS-712: Computer Forensics

Digital Forensic Tools and Resources

Baljeet Malhotra, PhD

Digital Forensic Tools and Resources

Name	Description	Status	URL
Exiftools	Metadata analysis	Active	https://exiftool.org/
Hashmyfiles	Hash analysis	Dormant	https://github.com/forenpackages/hashmyfiles
TRID	Signature analysis	Active	https://marko.net/soft-trid-e.html
Autopsy Forensic Analyzer	Data Carving, Analysis	Active	https://www.autopsy.com/
FTK Image, Arsenal Image Mounter, CAINE	Forensic Imaging & Mounting Image files	Active	https://www.caine-live.net/page11/page11.html
KAPE, Redline	Collection for Incident Response	Active	https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape
EricZimmerman Tools	Event Log Analysis	Active	https://ericzimmerman.github.io/
EricZimmerman Tools	Prefetch File Analysis	Active	https://ericzimmerman.github.io/
EricZimmerman Tools	MFT Parsing, timeline creation	Active	https://ericzimmerman.github.io/
Regripper	Registry Analysis	Dormant	https://github.com/keydet89/RegRipper3.0
EricZimmerman Tools	Jumplist, Link File	Active	https://ericzimmerman.github.io/
Timeline Explorer	Event Log Analysis	Active	https://ericzimmerman.github.io/
Volatility	Memory Forensics	Active	https://github.com/volatilityfoundation/volatility
Sysinternals	Live Forensics	Active	https://learn.microsoft.com/en-us/sysinternals/
MITRE ATT@CK	IR Framework	Active	https://attack.mitre.org/
WireShark	Packet analysis	Active	https://www.wireshark.org/

Digital Forensic Tools and Resources

Name	Description	Status	URL
EnCase Forensic	Collect/organize metadata from devices	Active	https://www.opentext.com/products/encase-forensic
ProDisccover Forensics	Collect/organize metadata from devices	Active	https://prodiscover.com/
ArcSight Logger	Digital Forensic tool by MicroFocus	Dormant	https://www.microfocus.com/documentation/arcsight/logger-7.2.2
Netwitness Investigator	Malicious Activity Detection	Active	https://www.netwitness.com/contact-us/netwitness-investigator-freeware/
Change Auditor	Active Directory tracker by Quest	Active	https://www.quest.com/products/change-auditor-for-active-directory-queries/
Forensic Toolkit (FTK)	Digital Forensic tool by AccessData	Dormant	https://accessdata-ftk-imager.software.informer.com/3.1/
Physical Analyzer	Digital Forensic tools by Cellebrite	Active	https://cellebrite.com/en/physical-analyzer/
Lantern	Katana Forensics for iPhone/iPod/iPad	Dormant	http://www.mobileforensicscentral.com/mfc/products/lantern.asp?pg=d&prid=387&pid=
WinHex	Data Recovery and Digital Forensics by X-Ways AG.	Active	https://www.x-ways.net/winhex/
National Software Reference Library (NSRL)	Database of hashed files managed by NIST	Active	https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl
Malware-Feed	Repository that contains actual malware	Dormant	https://github.com/MalwareSamples/Malware-Feed
Cutter	An advanced FREE and open-source reverse-engineering platform	Active	https://cutter.re/

Digital Forensic Tools and Resources

Name	Description	Status	URL
PEiD	PEiD detects most common packers, cryptors and compilers for PE files.	Dormant	https://www.aldeid.com/wiki/PEiD
Immunity Debugger	A powerful tool to write exploits, analyze malware, and reverse engineer binary files.	Active	https://www.immunityinc.com/products/debugger/
Ghidra	Open source reverse engineering tool developed by the National Security Agency (NSA) of the United States	Active	https://github.com/NationalSecurityAgency/ghidra
x64dbg	Dynamic analysis and debugging of executables	Active	https://x64dbg.com/
OllyDbg	Assembler-level analyzing debugger for Windows, commonly used for dynamic analysis and debugging	Dormant	https://www.ollydbg.de/
xiosec/Reverse-engineering	Repository that contains list of Reverse Engineering tools	Active	https://github.com/xiosec/Reverse-engineering
stego-toolkit	Collection of steganography tools - helps with CTF challenges	Dormant	https://github.com/DominicBreuker/stego-toolkit
Burp Suite	scanning for API vulnerabilities, manipulating requests, and analyzing responses.	Active	https://portswigger.net/burp/communitydownload
API Discovery	API Forensics, API Security and API Fraud Analysis	Active	https://apidiscovery.teejlab.com/edsn/knowledgebase/

Categorization of Forensic Tools

☐ **Imaging and Mounting**

- FTK Image
- Arsenal Image Mounter
- WinHex

☐ **Memory Forensic**

- Volatility
- ExifTools

☐ **Registry Analysis**

- Regripper
- Data Carving

☐ **Hash Analysis**

- HashMyFiles

☐ **Packet Analysis**

- WireShark
- API Discovery

Imaging and Mounting Tools

Provide the means to capture, preserve, analyze, and present digital evidence in a manner that is both efficient and legally acceptable. Their importance can be highlighted in several key aspects:

- ❑ **Preservation of Evidence:** Create exact bit-for-bit copies of digital media (hard drives, flash drives, etc.).
 - Capture all data on the device, including deleted files and unallocated space, forensic investigators can analyze all potential evidence.
- ❑ **Analysis Efficiency:** Enable analysis without the need for the physical media, which can be stored securely to prevent any tampering.
 - Mount the image as a drive on forensic workstation, and search for specific information and recover deleted or hidden files.
- ❑ **Non-Intrusive Examination:** Ensures state of the original evidence.
 - The non-intrusive approach is fundamental in digital forensics, as any modification to the original data could potentially compromise the case.
- ❑ **Time-Stamping and Logging:** Imaging and mounting tools often include features that log all actions taken during the forensic process.
 - Creates an audit trail that documents the integrity of the investigation, showing that the evidence was handled in a manner consistent with standards.
 - Time-stamping ensures that each step of the process is recorded, providing a chronological trail that can be important in legal proceedings.
- ❑ **Legal Admissibility:** Depends largely on the methods used to collect, analyze, and present evidence.
 - Imaging and mounting tools that follow accepted forensic standards help ensure that digital evidence is considered valid and admissible in court.
 - Help demonstrate that evidence has NOT been tampered with and that the procedures used are reliable and repeatable.
- ❑ **Versatility and Compatibility:** Compatible with a wide range of digital storage devices and file systems.
 - Crucial as investigators may encounter different devices and technologies.
- ❑ **Data Recovery and Analysis:** Recovery from damaged/formatted drives, decryption/encrypted files, and analysis of complex file systems.
 - Capability is essential for thorough forensic investigations where access to all possible data is necessary for uncovering the truth.

Memory Analysis Tools

Examining the volatile data in a computer's RAM (Random Access Memory) to uncover evidence that might not be found through traditional hard drive analysis. Information about running processes, open files, network connections, and potentially malicious code. Some of the key functions are:

- ☐ **Access to Volatile Data:** Data that are not stored on disk and would otherwise be lost upon power off or reboot.
 - Access data such as running processes, network connections, open files, and system and user memory.
- ☐ **Identification of Malicious Activities:** Many types of malware are designed to leave minimal footprints on persistent storage.
 - Detect and analyze malicious processes, including rootkits and memory-resident malware, providing evidence of compromise or attacks.
- ☐ **Recovery of Cryptographic Keys and Passwords:** Captures sensitive information like passwords, encryption keys, and other credentials.
 - These details aid in decrypting encrypted files or communications intercepted during investigations.
- ☐ **Real-time Incident Response:** Memory analysis is a critical component of identifying the scope of a breach or attack.
 - Allows quick identification of compromised systems, attacker methodologies, and containment of threats by analyzing the memory of live systems.
- ☐ **Timeline Analysis:** Help construct timelines of system and application activities.
 - Imaging and mounting tools that follow accepted forensic standards help ensure that digital evidence is considered valid and admissible in court.
 - Help demonstrate that evidence has NOT been tampered with and that the procedures used are reliable and repeatable.
- ☐ **Discovery of Ephemeral Data:** Reveal ephemeral data such as clipboard contents, data in transit, or the state of running applications.
 - Critical in investigations, offering insights into user actions and intentions.
- ☐ **Legal and Regulatory Compliance:** Crucial that an organization has taken measures to investigate and respond to security incidents.

Registry Analysis Tools

Play a crucial role in investigations involving Windows operating systems. The Windows Registry is a hierarchical database that stores low-level settings for the operating system and for applications that opt to use the Registry. The importance of Registry analysis tools can be summarized as follows:

- ❑ **Revealing System Information and Configuration:** Information about the configuration of the operating system
 - Including installed software, system settings, and hardware devices.
 - Detect changes made to the system, applications that were installed or removed, and the configuration of devices, which can be critical in an investigation
- ❑ **User Activities and Behavior:** Data on user profiles, login times, and network access.
 - Understand the actions taken by users on a system, potentially revealing intentions, habits, or evidence of malicious activity.
- ❑ **Tracking User Accounts and Login Activities :** Captures sensitive information like passwords, encryption keys, and other credentials.
 - Identify who accessed the system, when they accessed it, and what actions they may have taken.
- ❑ **Recovering Passwords and Decryption Keys:** Configuration data, including encrypted passwords or keys, within the Registry.
 - Recovering passwords or keys, provides access to encrypted files or communications.
- ❑ **Determining Program Execution :** Information related to program execution through, UserAssist, ShimCache, and RecentFileCache.bcf.
 - Determine what programs were run on a system, which is particularly useful in malware investigations and unauthorized software usage cases.
- ❑ **AutoStart Extensibility Points (ASEPs) Analysis:** Malware/applications use Registry keys to ensure their auto-execution.
 - Identify potentially malicious software that was intended to persist between reboots, aiding in malware detection and eradication.

Hash Analysis Tools

Fundamental for ensuring the integrity, authenticity, and non-repudiation of digital evidence. Generates unique digital fingerprints for files, data segments, or entire storage devices. Importance of hash analysis:

- ❑ **Integrity Verification:** Verifies that digital evidence has not been altered from the time of acquisition to its presentation in court
 - Comparing initial hash value of digital evidence with its current hash value, can confirm that the data remains unchanged, ensuring its integrity.
- ❑ **Identifying Known Files:** Rapid identification of known files, legal documents, or known illegal content (e.g., child exploitation material).
 - Use hash databases, like the National Software Reference Library (NSRL) database, to filter out known legitimate files from their investigations,
 - Helps on focusing on unknown or suspicious files, accelerating investigation process and aids in identifying illicit materials.
- ❑ **Detecting Duplicate Files:** Finding duplicate files across different devices or locations is crucial.
 - Identify duplicates by comparing hash values, which can indicate file copying, distribution of specific content, or the presence of backup/storage devices.
- ❑ **Evidence Correlation:** Correlate files and data across multiple devices and systems involved in an investigation.
 - Useful in complex cases involving multiple suspects or locations, where establishing links between different pieces of evidence is essential.
- ❑ **Data Recovery and Carving:** Hash analysis can verify the integrity of recovered files.
 - Ensures that the files are complete and have not been corrupted during the recovery process.
- ❑ **Malware Analysis:** Hash values of files can be compared against databases of known malware signatures.
 - Allows rapid identification of infected files or malicious software on a system.

Home Exercise - Case Studies



Real Case Studies

William Macquarie Case Study: <http://www.youtube.com/watch?v=vJdME6vczeo>

Bin Laden Forensic Case Study: https://www.youtube.com/watch?v=4W_P_Yxhnt0

OpenText Forensic Tools: <https://www.guidancesoftware.com/encase-forensic#digital>

Case Study - API Forensics



Agenda

❑ **Why API Forensics**

- Growing APIs
- Connected Systems

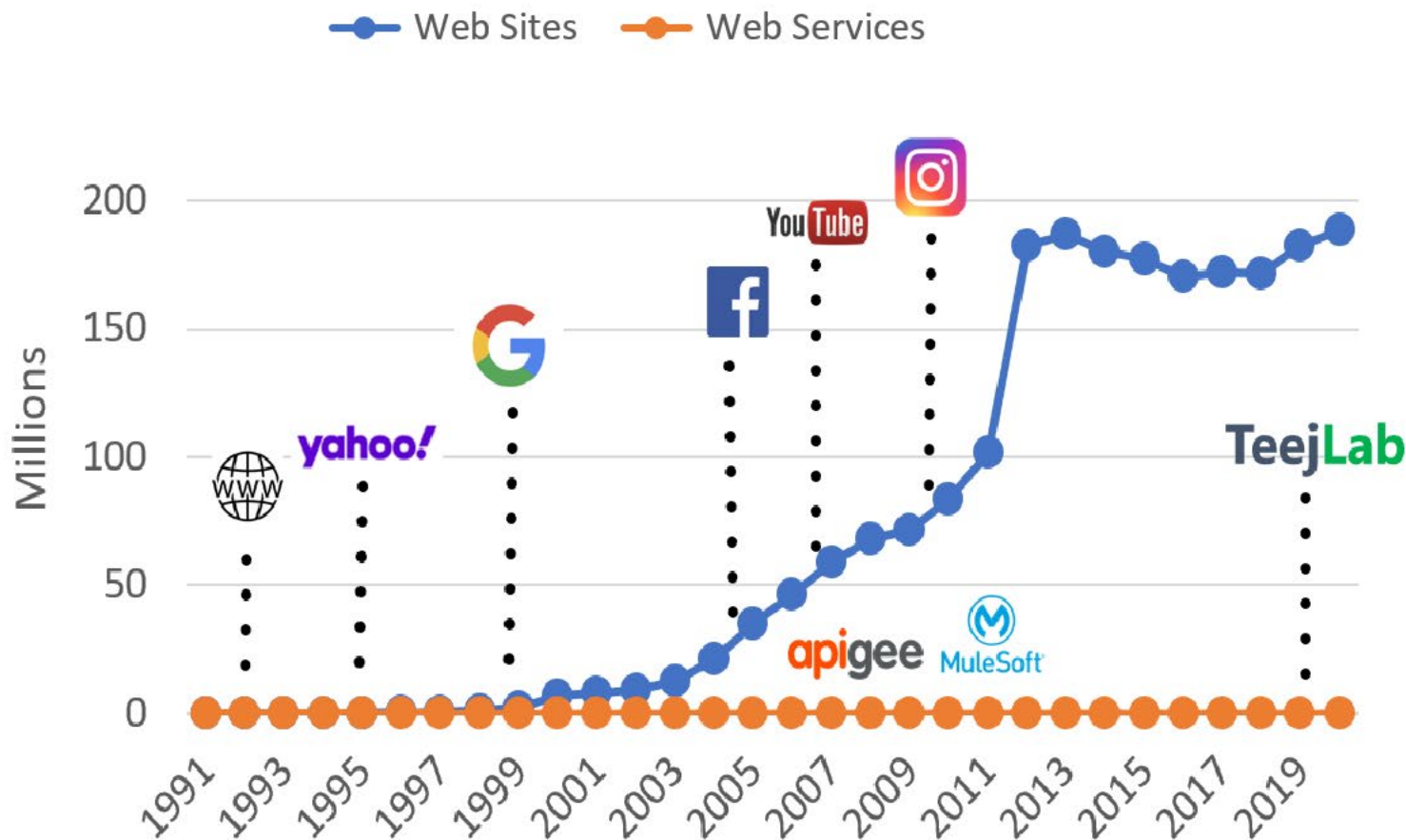
❑ **Challenges for API Forensics**

- Enterprise API Ecosystems
- Discovery of APIs
- API Authentications

❑ **API Forensics Process**

- Collecting Analytics
- Practicing examples

Why API Forensics ?



API is **common glue** of most web traffic, following Metcalf's law

83% of internet traffic via APIs vs 17% HTML! 1 Million Web APIs.

Enterprise moving rapidly towards **monetizing Digital Assets** via APIs

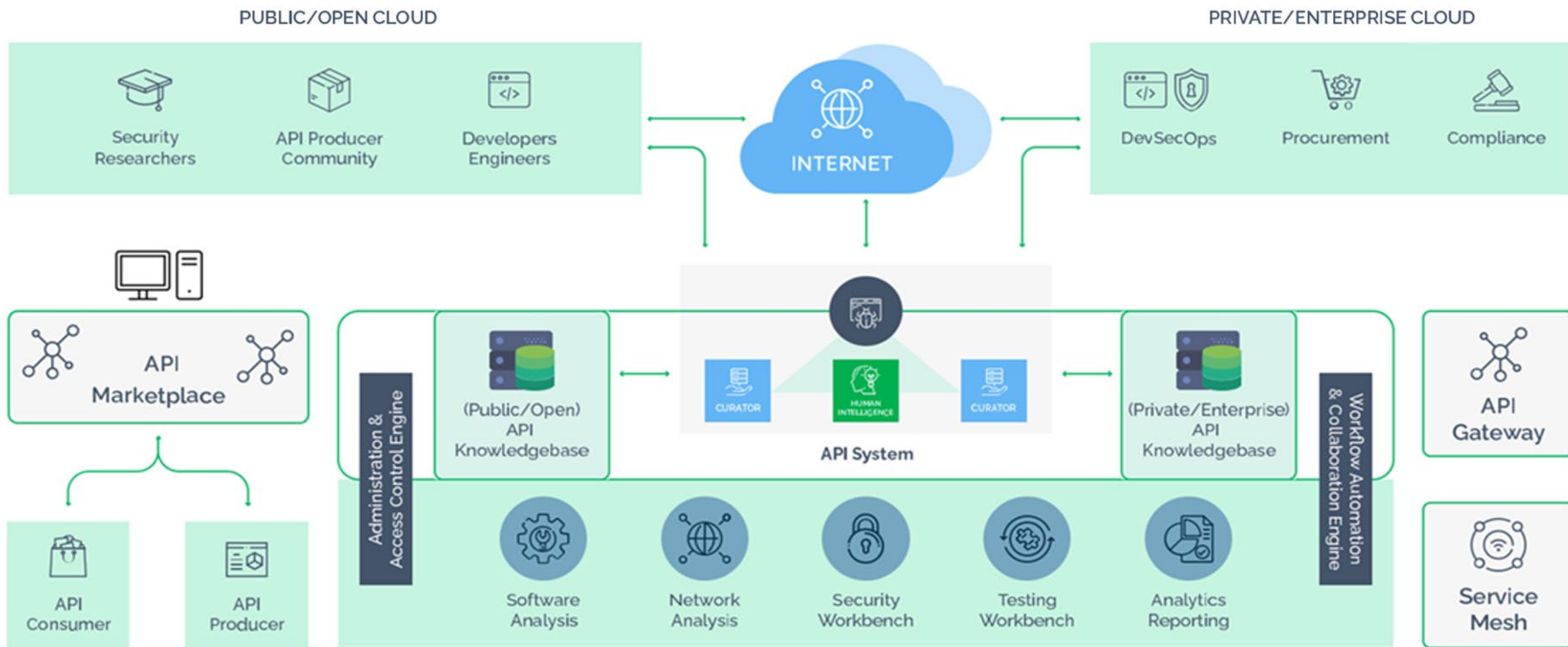
Smart devices, IoTs, AI/ML based economy primarily driven via APIs

APIs help **enterprises** to provide **automated intelligent** solutions.

APIs must be Discovered, Secured and Governed systemically.

Acknowledgement: Above demonstration/representation of an API Ecosystem is the copyright of TeejLab Inc.

API Forensic Challenges - Complex Enterprises



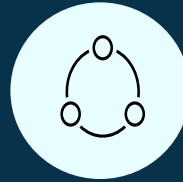
Acknowledgement: Above demonstration/representation of an API Ecosystem is the copyright of TeejLab Inc.

API Forensic Challenges - Variety and Volume



External APIs

- Centralize inventory
- Custodianship
- Access control
- License management
- Pricing management
- Continuous security check



Internal APIs

- Centralize inventory
- Custodianship
- Version control
- Access control
- Govern usage
- Centralize documentation



Unknown APIs

- APIs from Open Source
- APIs from M&A
- Security and quality
- Legal compliance
- Changing terms of service
- Continuous security checks

API Challenges - Authentication Problems

- Unprotected APIs that are “internal”
- Weak API keys that are not rotated
- Credentials and keys included in URLs
- Passwords that are default, weak, plain text, poorly hashed, shared
- Authentication susceptible to brute force attacks and credential stuffing
- Weak authentication that does not follow industry best practices
- Lack of access token validation (including JWT validation)
- Unsigned or weakly signed non-expiring JWTs

API Challenges - Authorization (Object Level)

- API call parameters use the ID of the resource accessed through the API */api/dept1/financial_info*.
- Attackers replace the IDs of their resources with a different one which they guessed through */api/dept2/financial_info*.
- The API does not check permissions and lets the call through.
- Problem is aggravated if IDs can be enumerated */api/123/financial_info*.

API Challenges - Authorization (Function Level)

- Administrative functions exposed as APIs.
- Non-privileged users accessing functions without authorization.
- Matter of knowing the URL, or using a different verb or a parameter:
 - */domain/api/users/v1/user/myinfo*
 - */domain/api/admins/v1/users/all*

Challenges of API Forensics - Summary

❑ Thousands of APIs

- What data APIs are exchanging
- Where APIs hosted (server/locations)
- Which teams/products use which APIs
- One team/product may use multiple APIs
- One API may be used in/by multiple products/team

❑ Hundreds of API Providers

- Vendors may provide free or commercial APIs
- Which APIs are more secure and compliant
- Terms of Use may change at any time

❑ Tens of API Tools and Processes

- Manage 100s of APIs specific test cases
- CIS top-20, OWASP top-10 security tests
- PCI, SOC2, HIPPA, ISO27001 compliance

Analytics for API Forensics

 API Inventory

 API Quality

 API Category

 API Trust

 API Age

 API License

 API Function

 API Risks

 API Vulnerabilities

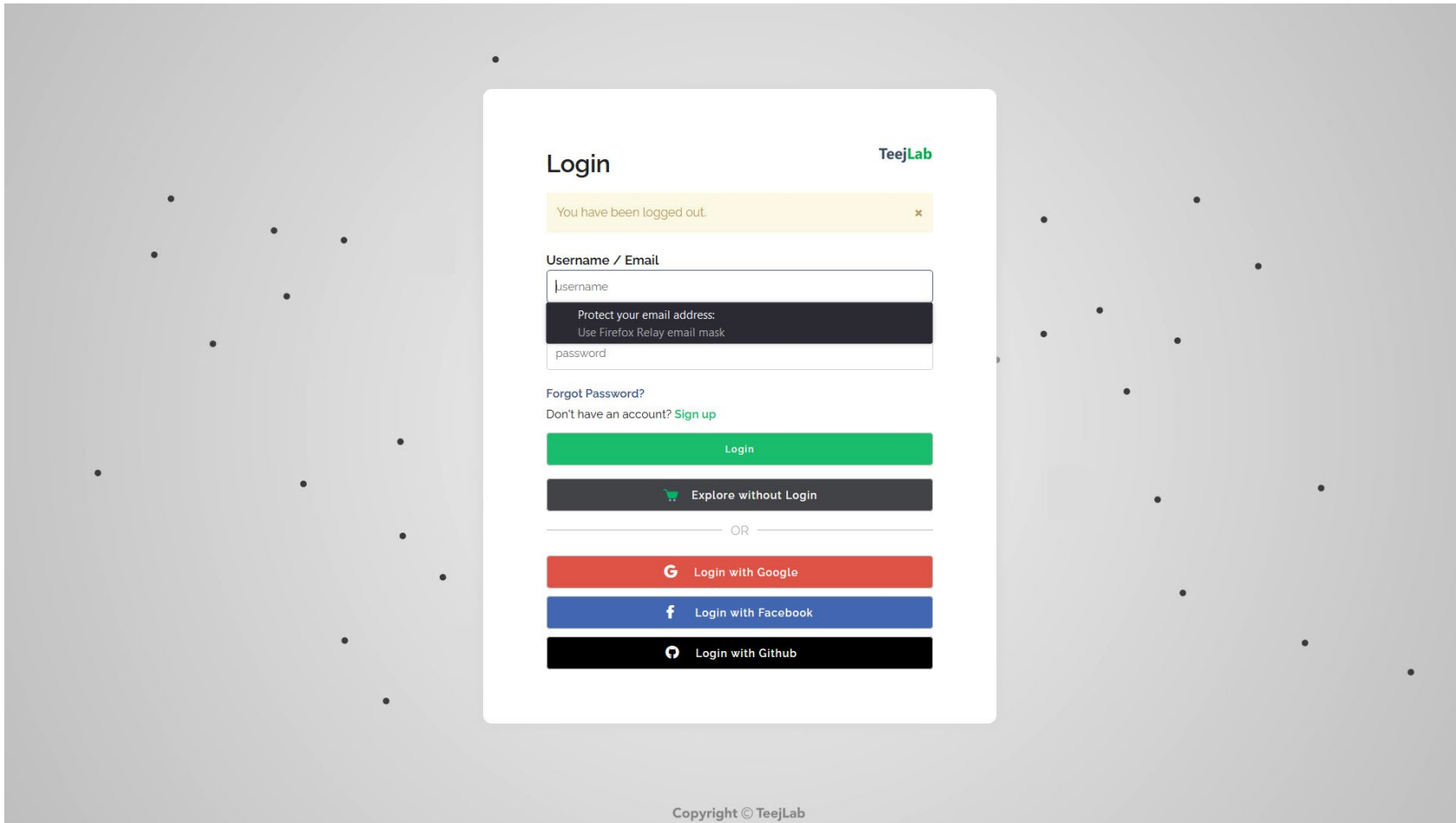
 API Health

Tools for Conducting API Forensics



API Discovery by TeejLab

Instructor will send an invite for to you sign-in
Sign-in using your NYIT email account

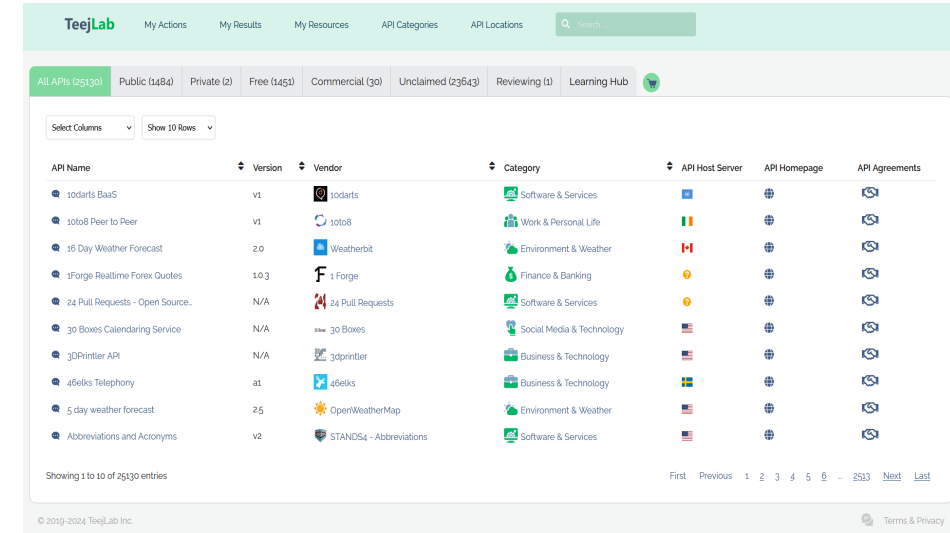


The screenshot shows the TeejLab login interface. At the top right is the 'TeejLab' logo. Below it is a yellow notification bar stating 'You have been logged out.' with a close button. The main section is titled 'Login' and contains a 'Username / Email' input field with a placeholder 'username'. Below this is a dark grey box with the text 'Protect your email address: Use Firefox Relay email mask'. A 'password' input field follows. There are links for 'Forgot Password?' and 'Don't have an account? Sign up'. A green 'Login' button is present, along with a dark grey button labeled 'Explore without Login' with a shopping cart icon. Below these is a horizontal line with 'OR' in the center. At the bottom are three social login buttons: 'Login with Google' (red), 'Login with Facebook' (blue), and 'Login with Github' (black).

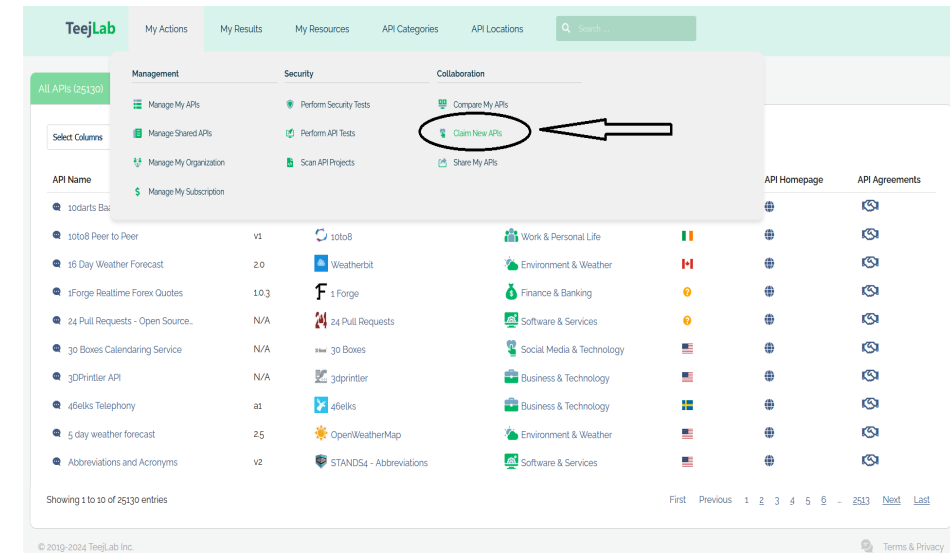
Copyright © TeejLab

Class Exercise or Online Assignment / Quiz

Step 1: Go to your API Discovery account



Step 2: Claim an API from Marketplace



Step 3: Conduct your analysis

API Forensics - Additional Resources

- **API Learning Hub:**
<https://apidiscovery.teejlab.com/edsn/learning>
- https://inria.hal.science/hal-01758692/preview/431606_1_En_11_Chapter.pdf
- <https://www.rule4.com/services/incident-response/api-forensics/>
- <https://indiaforensic.com/api-forensics-security/>
- <https://plugins.jenkins.io/forensics-api/>

A person wearing a grey hoodie is seen from behind, sitting at a desk. In front of them is a computer monitor displaying lines of code. The background is filled with a digital aesthetic, featuring a grid of binary code (0s and 1s) in green and blue tones. The overall lighting is dim and blue-toned, suggesting a nighttime or indoor digital environment.

INCS-712: Computer Forensics

Next - API Forensics (cont.)

Baljeet Malhotra, PhD