

Esta apresentação detalhada sobre **Computação Forense Móvel** baseia-se nas diretrizes e conhecimentos compartilhados por Benny Cleveland, um especialista com mais de duas décadas de experiência na área.

1. Princípios Fundamentais e Técnicas Iniciais

A base de qualquer investigação forense móvel confiável repousa em quatro pilares técnicos:

- **Cadeia de Custódia:** É essencial manter um registo seguro e documentado de cada etapa do manuseio da evidência. O uso de **sacos de Faraday** é crucial para bloquear o acesso à rede e evitar adulterações remotas.
- **Solidez Forense (Forensic Soundness):** Utiliza-se **bloqueadores de escrita (write blockers)** de hardware para garantir que nenhum dado seja modificado durante a extração. A integridade é verificada através de técnicas de *hashing* (MD5 ou SHA-256) antes e depois da extração.
- **Volatilidade de Dados:** Foca na captura de dados temporários, como o conteúdo da **memória RAM**, antes que sejam perdidos ao desligar o aparelho. Ferramentas como Belkasoft RAM Capturer e ADB são recomendadas para este fim.
- **Data Carving:** Técnica usada para recuperar arquivos deletados de áreas não alocadas do armazenamento, frequentemente utilizando a ferramenta **Autopsy**.

EC-Council | CyberTalks

Overview of Mobile Forensics Principles Techniques

The diagram illustrates the four pillars of mobile forensics:

- Chain of Custody:** Includes a checklist for evidence handling and a list of steps to secure the device.
- Forensic Soundness:** Focuses on protecting data integrity using hashing (MD5 or SHA-256) before and after extraction.
- Data Volatility:** Emphasizes acquiring volatile data (RAM) before the device is shut down, using tools like Belkasoft RAM Capturer and ADB.
- Data Carving:** Involves recovering deleted files and fragments from unallocated space using tools like Autopsy.

Dimension 2: Time of Deployment

Pre-Incident:

- Higher atomicity dump
- Requires forensight before incident occurs

Post-Incident:

- Can be used if incident has already occurred
- Lower atomicity dump

Autopsy Screenshot:

Volume	Layout	Type	File System	Status
Disk 0 (partition 0)	Simple	Basic	NTFS	Healthy (Boot, Page File, Cr)
Disk 0 (partition 1)	Simple	Basic	NTFS	Healthy (Recovery Partition)
Disk 0 (partition 2)	Simple	Basic	NTFS	Healthy (Recovery Partition)
Disk 0 (partition 3)	Simple	Basic	NTFS	Healthy (Recovery Partition)
RA DATA (F)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (G)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (H)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (I)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (J)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (K)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (L)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (M)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (N)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (O)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (P)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (Q)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (R)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (S)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (T)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (U)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (V)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (W)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (X)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (Y)	Simple	Basic	NTFS	Healthy (Primary Partition)
RA DATA (Z)	Simple	Basic	NTFS	Healthy (Primary Partition)

Chain of Custody

- Secure the device in a Faraday bag to prevent remote tampering or wiping via network communication.
- Document the handling of the device in real-time using evidence collection software.

Forensic Soundness

- Use hardware write blockers to ensure no data modification occurs during extraction.
- Verify data integrity using MD5 or SHA-256 hashing before and after extraction.

Data Volatility

- Acquire volatile data such as RAM and running processes before the device is shut down, using tools like Belkasoft RAM Capturer and ADB (Android Debug Bridge).

Data Carving

- Employ data carving techniques with tools like Autopsy to recover deleted files and fragments from unallocated space on a mobile device's storage.

<https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/>

2. O Processo de Investigação

O fluxo de trabalho forense segue etapas rigorosas para garantir que a evidência seja admissível em tribunal:

- **Reconhecimento do Dispositivo:** Identificação do modelo, sistema operacional, fabricante e inspeção de componentes externos como cartões SIM ou SD.
- **Localização da Evidência:** Identificação de todas as áreas de armazenamento, incluindo memória interna (NAND, eMMC), armazenamento externo e contas em nuvem vinculadas (iCloud, Google Drive).
- **Preservação da Integridade:** Criação de uma imagem forense do dispositivo e uso de valores de *hash* para validar que nada foi alterado.
- **Análise e Documentação:** Revisão de logs e descobertas, mantendo uma trilha de auditoria detalhada de todas as ferramentas e métodos utilizados.

EC-Council | CyberTalks

Key Principles of Mobile Forensics



Device Recognition

- Device Identification: Determine device model (smartphone, tablet), operating system (iOS, Android), and specific characteristics (manufacturer, version).
- Storage & Condition Check: Inspect for external storage (SIM, SD cards) and document visible physical conditions.



Evidence Location

- Storage Identification: Identify internal memory (NAND, eMMC) and check for external storage (SIM cards, SD cards).
- Cloud & App Storage: Locate cloud accounts (iCloud, Google Drive) and consider app-specific storage (encrypted containers, hidden files).



Data Integrity

- Data Preservation: Use write-blocking tools, create a forensic image, and verify integrity with hash values (MD5, SHA-256).
- Analysis & Documentation: Perform analysis on the forensic image and maintain chain of custody records.



Chain of Custody

- Action Logging: Record every action taken with the device, including access times and personnel involved.
- Maintain Integrity: Keep detailed documentation to preserve the evidence's legal admissibility.

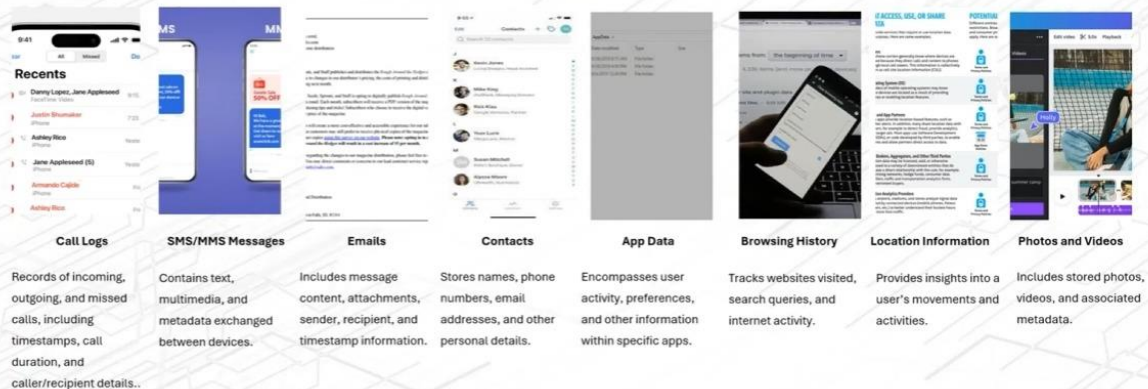
<https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/>

3. Tipos de Dados e Técnicas de Extração

Os investigadores buscam diversos tipos de dados para construir uma narrativa cronológica:

- **Dados de Comunicação:** Registros de chamadas, SMS/MMS, e-mails e listas de contatos.
- **Atividade Digital:** Histórico de navegação, dados de aplicativos (hábitos e preferências) e informações de localização (GPS e Wi-Fi).
- **Mídia:** Fotos e vídeos, que contêm metadados cruciais como data, hora e etiquetas de localização.

Mobile Data Types



<https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/>

Para extrair esses dados, utilizam-se métodos **lógicos, físicos e de sistema de arquivos**. A extração em nuvem permite recuperar dados sincronizados que podem não estar presentes localmente no dispositivo.

Mobile Data Types and Extraction Techniques Cont'd



<https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/>

4. Ferramentas Avançadas e Acessórios

A escolha da ferramenta depende do objetivo da investigação:

- **Cellebrite UFED:** Considerada uma solução completa para extração versátil de dispositivos e nuvem.

- **Magnet Axiom:** Destaca-se pela análise profunda, correlação de dados e visualização de padrões.
- **MSAB XRY:** Focada em velocidade e integridade, com capacidades de descriptografia de arquivos bloqueados.
- **Elcomsoft Phone Breaker:** Especializada em contornar criptografia e autenticação de dois fatores (MFA) para dados em nuvem.
- **MOBILedit Forensic:** Preferida para a criação de relatórios estruturados e prontos para o tribunal.

Além do software, são necessários acessórios como **leitores de cartão SIM/SD, cabos especializados, adaptadores de unidade NVMe/SATA e isoladores de rede forense.**

Mobile Device Forensics Accessories



Write Blocker



Specialized Cables and Adapters



Faraday Bag



SIM and SD Card Readers



External Hard Drives and Storage Devices

<https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/>

13

Mobile Device Forensics Accessories Cont'd



Power Adapters and Portable Power Banks



SATA to USB Adapter and an NVMe Drive Adapter

Forensic Network Isolator



Forensic Phone Cables

<https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/>

14

5. Táticas para Aplicativos e Nuvem

As fontes detalham procedimentos técnicos avançados para lidar com a complexidade dos dados modernos, que frequentemente estão protegidos por criptografia ou distribuídos em ambientes de rede.

Abaixo, detalho as estratégias específicas para aplicativos, redes sociais e ambientes de nuvem:

5.1. Recuperação Profunda de Aplicativos de Mensagens

Para aplicativos como **WhatsApp e Signal**, que utilizam criptografia de ponta a ponta, o processo de investigação segue etapas rigorosas para transformar dados brutos em evidências legíveis:

- **Aquisição e Extração:** O dispositivo é conectado a uma estação de trabalho forense usando **bloqueadores de escrita** para garantir a integridade. Ferramentas como o **Cellebrite UFED** ou **Magnet AXIOM** realizam extrações lógicas ou físicas para atingir bancos de dados brutos, como o `msgstore.db` do WhatsApp.
- **Descriptografia e Parsing:** Uma vez extraídos, os dados podem exigir técnicas de quebra de senha ou o uso de capacidades nativas das ferramentas forenses para descriptografar o conteúdo. Após isso, navegadores de banco de dados (como o **SQLite**) são usados para analisar logs de chat, carimbos de data/hora e mídias compartilhadas

EC-Council CyberTalks

Mobile Application Forensic Tactics



Messaging App Data Recovery

Extracting and decrypting chat logs, attachments, and metadata from encrypted messaging apps like WhatsApp and Signal using tools like Cellebrite UFED or Magnet AXIOM.

Database Analysis

Analyzing databases like `msgstore.db` for WhatsApp to recover messages, contacts, and shared media, including deleted items.

Forensic Extraction

Using mobile forensic tools to extract data from suspect's device, including encrypted chat logs, attachments, and metadata.

Encrypted Communication Tracking

Investigating suspect's use of encrypted messaging apps to communicate and track their activities.

<https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/>

- **Recuperação de Deletados:** Através da análise da **memória não alocada** do dispositivo, investigadores podem recuperar fragmentos de mensagens que foram apagadas pelo usuário, mas que ainda não foram substituídas pelo sistema.

5.2. Forense em Redes Sociais (Facebook e Instagram)

A investigação de redes sociais não se limita ao que é visível no perfil público, focando em dados armazenados localmente no aparelho:

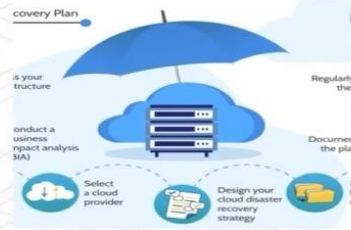
- **Análise de Cache Local:** Investigadores extraem arquivos de cache (como o `cache.db`), que podem conter imagens, comentários e perfis visualizados recentemente, mesmo que tenham sido alterados ou removidos da conta principal.
- **Tokens de Sessão:** A extração de tokens de login permite que investigadores acessem a conta vinculada na nuvem sem precisar das credenciais originais, possibilitando a visualização de mensagens privadas e conexões de amigos diretamente do servidor do provedor.

5.3. Táticas Avançadas e Desafios de Nuvem

A computação forense em nuvem expande o alcance da investigação para além do hardware físico:

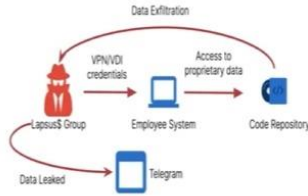
- **Réplicas e Shadow Copies:** Utiliza-se réplicas na nuvem e "cópias de sombra" para restaurar versões anteriores de arquivos que podem ter sido perdidos ou criptografados por criminosos
- **Contorno de MFA e Criptografia:** Em casos onde o acesso é negado, técnicas avançadas são empregues para ignorar a **Autenticação de Múltiplos Fatores (MFA)** para obter acesso autorizado a dados vitais para o caso. Segundo o especialista Benny Cleveland, a **Inteligência Artificial** será uma aliada no futuro para lidar com esses múltiplos rounds de criptografia.

Mobile Application Forensic Tactics Cont'd



Cloud Replicas and Shadow Copies for Data Recovery

Utilize cloud replicas and shadow copies to restore previous versions of files and recover lost or encrypted data.



Bypassing Encryption and MFA for Cloud Data Access

Use advanced forensic techniques to bypass encryption and multi-factor authentication (MFA) to gain authorized access to cloud-stored data when necessary for investigation.



Navigating Cross-Border Data Laws in Cloud Forensics

Ensure compliance with international data protection regulations (e.g., GDPR, CCPA) when handling cloud data across different jurisdictions during forensic investigations.

<https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/>

17

Cloud Forensic Tactics



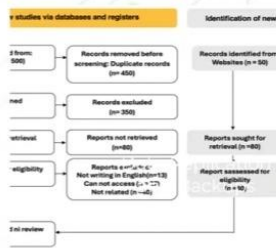
Extracting Mobile Backups and Documents

Extracting mobile backups and documents involves retrieving and accessing stored data from mobile devices for analysis, recovery, or forensic purposes.



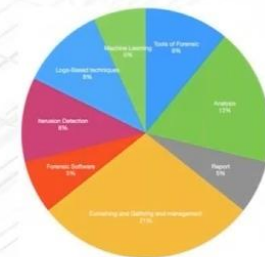
Malware Detection and User Activity

Malware detection and user activity monitoring involve identifying malicious software and analyzing user behaviors to safeguard systems from security threats and ensure compliance.



Tracking Access and Usage in Cloud Apps

Tracking access and usage in cloud apps involves monitoring user interactions and permissions to ensure security, compliance, and efficient resource management within cloud environments.



Tracking File Activity in Cloud Storage

Tracking file activity in cloud storage involves monitoring actions such as file creation, modification, sharing, and deletion to ensure data security, compliance, and proper access control.

<https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/>

20

- **Leis Transfronteiriças:** O investigador deve navegar por complexidades legais internacionais, como o **GDPR** (Europa) e a **CCPA** (Califórnia), ao lidar com dados armazenados em jurisdições diferentes daquela onde ocorre o crime.

5.4. Fluxo de Investigação de Violação de Dados (Cloud Breach)

Quando ocorre uma invasão em larga escala em ambientes de nuvem, as fontes descrevem um protocolo sistemático de seis etapas:

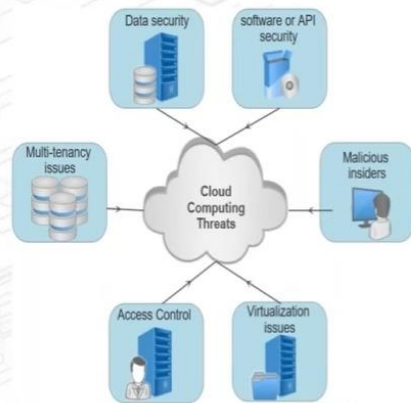
1. **Revisão de Logs de Acesso:** Identificar usuários, localizações e padrões anômalos de acesso.
2. **Análise de Metadados:** Examinar padrões de modificação ou exclusão de arquivos
3. **Exame de Autenticação:** Analisar logs para detectar credenciais comprometidas ou tentativas de login suspeitas.
4. **Análise de Snapshots e Backups:** Revisar o estado dos dados antes da violação para entender a extensão do dano.
5. **Análise de Logs de API:** Investigar se os invasores exploraram vulnerabilidades em APIs para interagir com os recursos de nuvem.
6. **Conclusão e Recomendações:** Sintetizar as descobertas e propor melhorias nos controles de acesso.

5.5. Estudo de Caso: Ataque de Ransomware (Ex: Garmin)

As fontes citam o ataque à Garmin como um exemplo de como a forense de nuvem lida com ransomware:

- A investigação envolveu a criação de snapshots de Máquinas Virtuais (VM) para preservar o estado do sistema antes e depois da infecção.
- As equipes realizaram a engenharia reversa do payload do ransomware para entender seu comportamento, origem e vulnerabilidades que pudessem ajudar na descriptografia dos dados.
- A recuperação foi tentada através de recursos de versionamento e backups baseados em nuvem.

Forensic Investigation Example 3 – Data Breach in Cloud Storage



Step 1

Access Logs Review

Retrieve cloud access logs to identify users and locations involved in data access.

Step 2

Metadata Analysis

Examine file metadata to understand access, modification, or deletion patterns.

Step 3

User Authentication Examination

Analyze authentication logs for compromised credentials or suspicious login attempts.

Step 4

Snapshot and Backup Analysis

Review cloud snapshots and backups to determine the state of the data before the breach.

Step 5

API Log Analysis

Investigate API logs for unauthorized access or exploitation of cloud resources.

<https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/>

22

6. Considerações Éticas e Legais

A conduta do investigador deve ser irrepreensível para garantir a validade do processo:

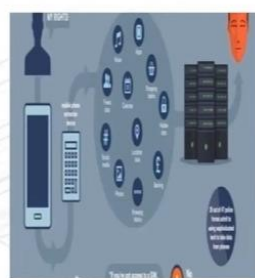
- **Mandado Legal e Consentimento:** Nenhuma análise deve começar sem autorização legal apropriada.
- **Minimização de Dados:** Coletar apenas o que é relevante para a investigação para respeitar a privacidade do indivíduo.

Legal and Ethical Considerations for Mobile Device Forensics



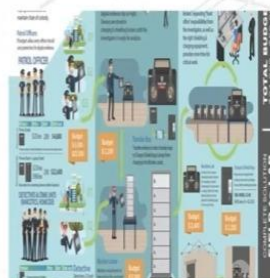
Legal Warrants and Consent

Ensure proper legal warrants or consent is obtained before accessing or analyzing data from mobile devices to avoid violating privacy laws.⁹



Privacy and Data Protection

Respect user privacy by limiting data collection to only the relevant information necessary for the investigation, in compliance with regulations like GDPR or CCPA.



Chain of Custody

Maintain a strict chain of custody for mobile devices and extracted data to ensure the integrity and admissibility of evidence in court.



Data Minimization

Apply the principle of data minimization by avoiding excessive data collection that is unrelated to the investigation, reducing the risk of overreach.

<https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/>

23

- **Verificação de Propriedade:** Confirmar quem é o dono do dispositivo antes do exame.
- **Padrões da Indústria:** Aderir a diretrizes reconhecidas como as da **NIST** ou **ISO** para manter a credibilidade.

EC-Council | CyberTalks

Legal and Ethical Considerations for Mobile Device Forensics Cont'd



Encrypted Data Handling

Ethically handle encrypted data, ensuring that efforts to bypass encryption do not violate the rights of individuals or breach legal standards.



Cross-Jurisdictional Issues

Address cross-border legal requirements when analyzing mobile data, as different countries have varying laws regarding data access, storage, and transfer.



Device Ownership Verification

Verify device ownership before conducting a forensic analysis to ensure that consent or legal authorization is obtained from the appropriate party.



Industry Standards Adherence

Follow industry-accepted forensic guidelines and practices (e.g., NIST, ISO) to ensure ethical, accurate, and defensible forensic analysis.

<https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/>

Conclusão e Insights (Q&A)

Durante a sessão, foi destacado que a **Inteligência Artificial (IA)** aumentará significativamente a eficiência das investigações, embora a habilidade do investigador humano continue sendo fundamental para análises físicas. Em casos de **ransomware**, o dispositivo deve ser isolado imediatamente antes de proceder com a recuperação de dados através de backups em nuvem ou snapshots